2011

Securing the Homeland: A Risk-Cost-Benefit Analysis of U.S. Anti-Terrorism Expenditures

Anne-Elise Martin
Claremont McKenna College

Securing the Homeland:

A Risk-Cost-Benefit Analysis of U.S. Anti-Terrorism Expenditures

By: Anne-Elise Martin

Adviser: Professor Mark Blitz

Introduction

In 2009-2010, the number and pace of attempted terrorist attacks against the United States surpassed any year since 9/11.[1] Three transnational terrorist groups launched nearly successful attacks against the U.S.: (1) a plot against the New York City subway system; (2) an attempt to blow up a Detroit-bound plane on Christmas Day; and (3) an attempt to detonate an improvised explosive device inside a vehicle parked in Times Square. In addition to these three incidents, there were also two successful "homegrown" terrorist attacks executed by individual U.S. citizens, Major Nidal Hassan and Carlos Bledsoe.

These events demonstrate the enduring capacity of terrorists to attack the United States despite America's extensive, well-funded security apparatus. Former U.S. Secretary of Homeland Security, Michael Chertoff, identifies two objectives for domestic security policy: first, to "manage rather than eliminate risks;" and second, to "engage in preparedness planning so that when disasters do happen, we can respond in a manner that minimizes the consequences."[2] When these two objectives are considered in light of the continuing barrage of terrorist plots and attacks against the United States, a question becomes obvious: Is the United States homeland security strategy effective?

This seemingly simple question is actually quite complex. The only way to even consider it is to first define an "effective" strategy. Effective does not mean perfect. It is impossible to detect and prevent every conceivable terrorist attack, and even if it were

---

[1] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.

[2] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.

possible, it would be inefficient and unsustainable to do so. Rather, an effective anti-terrorism strategy is essentially a pragmatic risk-cost-benefit analysis, whereby homeland security funds are allocated based on threat-specific cost-benefit analyses done in relation to actual risk. To be effective, anti-terrorism efforts must reflect *realizable* risk to U.S. homeland security—as opposed to politicized, exaggerated derivatives of risk often propagated by politicians and media.

Once an effective strategy is defined as action (cost) in proportion to actual risk and security benefit, it is then helpful to divide the primary question—is the U.S. homeland security strategy effective? — into three subsidiary questions. First, what are the current threats, including actors, modes of terrorism, and potential targets, to U.S. homeland security? Second, how does the United States address each of these threats, both in terms of programs and expenditures? And, third, taking into account actual risk, are the costs (meaning monetary expenditures, as well as, negative social and economic externalities from security measures) and the corresponding benefits (meaning gains in U.S. homeland security resulting from specific anti-terrorism programs) in equilibrium? Reaching this equilibrium point between risk, cost, and benefit is both a necessary and a sufficient condition for an effective U.S. homeland security strategy to mitigate risk and prepare the nation for potential disasters.

Chapter One: Risk

Risk, for the purpose of this paper, is defined as "the desire to gauge the likelihood of something being a hazard, and to project the possible outcomes should they occur, so that the costs and benefits of mitigating, risk-reducing measures can be assessed."[3] To be clear, hazards are anything that endangers society as a whole, and are typically broken up into two groups: naturally occurring and man-made. Hazards associated with terrorism are man-made, thus this paper will consider only man-made hazards. The Department of Homeland Security (DHS) uses a definition of risk that is comprised of three components: threats, vulnerabilities, and consequences;[4] and for this reason, the threat analysis below will address these three components of risk. This section will not detail the existing programs that address each threat, as the next section does, but merely considers the threat itself since "the first step in preventing or mitigating the risk of disaster is to know and understand the dangers we face."[5]

To begin with, Chapter One outlines the terrorist groups posing the greatest risk to U.S. homeland security. It then describes the various weapons technologies that may be used in a future attack. In addition, this chapter also provides an overview of other vulnerabilities to U.S. security, including cyber infrastructure, cargo and human transportation systems, and the U.S. energy system. Finally, this chapter contextualizes the current terrorist threat by considering trends in terrorist attacks over time.

---

[3] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[4] Ibid.
[5] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.

Terrorist Groups

Historically, terrorist groups fit into at least one of the following ideological categories: religious, nationalist/separatist, left and/or revolutionary, right and/or reactionary, anti-globalizationist, and extreme environmentalist. In the United States, the popular narrative to conceptualize terrorism and anti-U.S. terrorist activity frames terrorism as predominately, if not exclusively, religious. There are, however, timely examples of each of the other ideological categories as well. For example, the Palestinian Liberation Front (PLO) and the Basque group, Euzkadi Ta Askatasuna (ETA), are nationalist/separatist organizations; the Revolutionary Armed Forces of Columbia (FARC) is a left/revolutionary group; the Self Defense Forces of Columbia (AUC) is a right/reactionary organization; the Mexican Fuerzas Armadas Revolutionaries del Pueblo (FARP) is motivated by an anti-globalization ideology; and the Earth First and Earth Liberation Front organizations are environmental extremist.[6]

As evidenced by this litany of terrorist groups with disparate motivations and ideologies, it is more useful to consider the threat posed by various terrorist organizations on a group-by group basis than to consider the threat of specific ideologies (e.g. religious extremism), as is often done by policy analysts. To be clear, categorizing terrorist groups by ideological motivations may be more helpful than considering individual groups for a predictive analysis of the future of terrorism. For that sort of forward looking analysis the focus is preventing terrorism, unlike this paper, which functions as a snap shot of existing terrorist threats. For this reason, the following analysis examines individual terrorist groups posing a significant, realizable threat to U.S. homeland security.

[6] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.

Al Qaeda (AQ)

Michael Chertoff calls al Qaeda (AQ) the "most potent representative"[7] of extremist ideology today, while Vice-Admiral J. Michael McConnell, former U.S. Director of Intelligence, describes AQ as "the pre-eminent threat against the United States, both here and abroad."[8] AQ creates tremendous risk for U.S. homeland security because of the organization's extreme anti-American ideology, its willingness and ability to use a variety of weapons technologies, and because of the geographically dispersed network of its operations and affiliates that open new theatres of conflict in at least Afghanistan, Pakistan, Yemen, Somalia, and Iraq.

The threat of AQ attacks continues to evolve as the network's structure responds to counterterrorism efforts, specifically those in Afghanistan. Before 9/11, AQ had a stable base of operations in Taliban-controlled areas of Afghanistan, allowing the organization to assume a formal internal hierarchy and to create permanent installations and training camps.[9] In fact, one RAND Corporation study attributes AQ's successful attacks on 9/11, as well as their 1998 attacks in Kenya and Tanzania, to the stability afforded by a secure base of operations, internal hierarchy, and permanent installations.[10] AQ's organizational stability was compromised when the United States launched Operation Enduring Freedom, a military assault against the Taliban regime in

[7] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.
[8] Ibid.
[9] Chalk, Peter, et al. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*. *RAND Corporation*. Center for Terrorism Risk Management Policy. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf>
[10] Ibid.

Afghanistan, shortly after 9/11.[11] Operation Enduring Freedom scattered core AQ leadership to various locations in the Middle East, thereby decentralizing AQ planning and training efforts.

AQ organizational hierarchy has also been dramatically changed because key members have been captured or killed by U.S. and coalition forces. Examples of senior AQ leadership who have been eliminated or detained include: 9/11 coordinator, Ramzi bin al-Shibi; operational planners, Mohammed Atef, Abu Zubayduh, and Khaled Sheikh Mohammad; a senior leader of AQ on the Arabian Peninsula and organizer of the 2000 attack on the *USS Cole*, Adb al-Rahim al-Nashirih; AQ's foremost connection to Southeast Asian militant groups and the architect of the 2002 Bali attacks in Indonesia, Riduan Isamuddin; a major factor in the 1998 embassy attacks in Kenya and Tanzania, Ahmed Khalfan Ghalani; AQ's third most senior leader, as of 2005, and operational coordinator for Pakistan, Abu Faraj al-Libbi; and an important leader in disseminating AQ jihadist communications worldwide, Haitham al-Yemeni. [12]

AQ has also suffered major financial losses, totaling at least $136 million, in frozen or seized assets.[13] Additionally, a campaign to disable AQ's international fundraising efforts has "forced AQ to progressively adapt its jihadist 'business model' and switch to more secure, but less lucrative localized collection methods."[14] The loss of existing assets, coupled with an encumbered ability to collect international resources, weakens AQ's ability to execute large-scale terrorist attacks.

---

[11] Chalk, Peter, et al. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*. *RAND Corporation*. Center for Terrorism Risk Management Policy. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf>
[12] Ibid.
[13] Ibid.
[14] Ibid.

Another result of U.S. and coalition involvement in Afghanistan after 9/11 is the decentralization of AQ's institutional composition; "The loss of a secure haven in Afghanistan and the loss of key human capital resources have stripped the group of the vital command, logistical, and functional assets needed to operate in a vertically organized manner."[15] Since the U.S. invasion of Afghanistan, AQ has been forced to transition from centrally organized attacks executed by the group's core membership, to a more horizontal structure in which attacks are executed by geographically dispersed affiliates or individuals. This new structure, often referred to as a "movement of movements," is still motivated by a monolithic message of international jihad, but is now "nebulous, segmented, and polycentric in character."[16]

The nature of future AQ attacks will be markedly different as a result of the organization's structural and economic setbacks. Specifically, the RAND Corporation predicts four trends relating to future AQ attacks. First, AQ will shift from hard (meaning well-protected) targets to soft targets. Previous AQ attacks, like those on 9/11, have focused on hard targets to maximize the psychological impact of the attack and to demonstrate AQ strength as both a coercive and recruiting tactic. The United States took extensive measures after 9/11 to harden critical infrastructure deemed most vulnerable to terrorist attack; unfortunately, when targets are hardened, threat displacement occurs, and soft targets (meaning largely unprotected and publicly accessible venues) are left vulnerable. Soft targets are attractive because they are often densely populated, and thus an attack would likely yield mass causalities. The second trend identified by RAND, is

---

[15] Chalk, Peter, et al. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act. RAND Corporation*. Center for Terrorism Risk Management Policy. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf>

[16] Ibid.

that AQ will increasingly pursue economic attacks, regardless of the ability for such attacks to produce mass causalities. Economic attacks target major finical institutions (such as the World Trade Center), disrupt major supply chains (such as an attack against a U.S. sea port), expose risk and thus result in a massive reaction (such as a commercial airline strike resulting in new security regulations).

The third predicted AQ trend is a continued reliance on suicide attackers. Importantly, as domestic (homegrown) terrorism increases, the potential for suicide missions in the United States grows as single-actor operatives proliferate. Finally, the fourth anticipated trend is that AQ will continue to pursue chemical, biological, radiological, and nuclear (CBRN) weapons. Without question, AQ has shown interest in acquiring or building CBRN weapons. Though there is general consensus that AQ does not have nuclear weapons technologies, it is uncertain whether the organization has the ability to produce radiological, biological and chemical weapons, or the degree of sophistication to which such weapons can be produced. It is likely that the group has some ability to produce radiological, biological and chemical weapons, and thus, it is not unreasonable to assume that future AQ attacks will incorporate those weapons.

Aside from predictions of potential AQ attack trends, it is necessary to mention the threat posed by the group's ability to proliferate recruiting materials using a variety of media. AQ propaganda has already influenced the radicalization of extremists at home and abroad. For example, the 2009 Fort Hood shooter, Major Nidal Hassan, communicated with Anwar al-Awlaki, a former Imam and current AQ leader, whose use of new media technology to propagate AQ ideology worldwide has been linked to numerous attacks against the U.S. in recent years. Propaganda does more than recruit

sympathizers to the AQ cause; it is a force multiplier in that it encourages "like-minded extremists to conduct smaller-scale independent attacks that are inspired, but not overseen or directed, by the group."[17] The advent of new media recruiting allows would-be terrorists to connect with AQ without traveling to the Middle East, which makes detection more reliant on cybersecurity. In sum, threats from AQ to U.S. homeland security emanate from that organization's propaganda, and originate from both within and outside the United States. These threats could take the form of catastrophic terrorism, but will more likely involve small-scale attacks on soft targets or economically important nodes.

AQ Affiliates and Allies

Al Qaeda in the Arabian Peninsula (AQAP)

Since 2009, AQAP has emerged as one of the world's most lethal terrorist networks, with a demonstrated and resilient ability to recruit and train operatives, plan attacks, and facilitate the movement of terrorists from its home base in Yemen. AQAP's targets are international in scope. For example, in 2009 AQAP attempted to assassinate Saudi Prince Mohammed bin Nayef, and also attempted to blow up a Detroit-bound plane on Christmas Day. Importantly, Anwar al-Awlaki, mentioned above as a key communicator for AQ, is a member of AQAP and a dual Yemeni-American citizen. Al-Awlaki influenced Umar Farouk Abdulmutallab, the young man who attempted to blow up the plane, and has also been linked to numerous other terrorist attacks as a spiritual

[17] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.

leader and liaison between AQAP and individual recruits. AQAP continues to circumvent anti-terrorist efforts and will remain a prevalent threat to U.S. Homeland security.

Al Qaeda Operatives in Somalia and Al-Shabaab

There are numerous AQ operatives, as well as the Somalia-based terrorist and insurgent group, al-Shabaab, located in East Africa. Al-Shabaab was responsible for the July 2010 suicide bombings in Kampala, Uganda that killed 76 people. The group is also believed to be responsible for the 2008 suicide attacks against the United Nations and local government targets in northern Somalia. Al-Shabaab publicly supports AQ and Osama bin Laden, and shares aspects of AQ ideology; but al-Shabaab ideology is also Somali-nationalist. Al-Shabaab operates in collaboration with a small number of AQ operatives in East Africa to facilitate a terrorist training program created by al-Shabaab and the recently deceased AQ operative, Saleh Nabhan.[18] This camp attracts violent extremists from all over the world, including recruits from the United States—since 2006, at least twenty U.S. citizens have traveled to Somalia to fight and train with al-Shabaab.[19]

When testifying before the Senate Homeland Security and Government Affairs Committee in September 2010, Michael Leiter, the director of the National Counterterrorism Center, said "Within the last two months, four U.S. citizens of non-Somali descent were arrested trying to travel to Somalia to join al-Shabaab."[20] In addition, Leiter noted that U.S. citizen, Omar Hammami, traveled to Somalia in 2006 and

[18] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[19] Ibid.
[20] Ibid.

is now one of al-Shabaab's senior leaders.[21] Leiter also pointed out that, when interviewed by the New York Times, Hammami called the U.S. a legitimate target for future al-Shabaab attacks. Though not as grave a threat as AQ and AQAP, al-Shabaab remains a threat to U.S. homeland security.

Al Qaeda in the Lands of the Islamic Maghreb (AQIM)

AQIM is a terrorist group located in North and West Africa. The group has historically focused on kidnapping and small-arms attacks. Recently, however, AQIM has demonstrated the ability and intention to progress to more lethal attacks. In July, 2010, AQIM executed a French hostage and earlier that year, the group launched its first suicide bombing attack in Niger. The efforts of Algerian authorities have disrupted and deterred AQIM plots for mass-causality attacks, but the group's public support of Nigerian extremists and its ongoing plans to attack France demonstrate AQIM commitment to violence. Though not currently directed at the United States, AQIM is still a threat to U.S. citizens abroad and to U.S. interests in North and West Africa.

Al Qaeda Iraq (AQI)

AQI has continued to execute attacks within Iraq, despite counterterrorism efforts that resulted in the deaths of AQI's most senior leadership, including Abu Ayyub al-Masri, Abu Omar al-Baghdadi, Abu Khalaf, and Abu Abd al Rahman.[22] U.S. officials

[21] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[22] ROGGIO, BILL. "Senior al Qaeda in Iraq leader killed in Miqdadiyah." *The Long War Journal*. 16 Jan. 2008. Web. 31 Mar. 2011.<http://www.longwarjournal.org/archives/2008/01/senior_al_qaeda_in_i_1.php>.

describe AQI as "a numerically small but operationally major component of the Sunni Arab-led insurgency that frustrated U.S. efforts to stabilize Iraq."[23] After the U.S. "troop surge" in 2007, AQI was displaced from operational centers in Iraq, particularly in Baghdad and in Anbar Province.[24] U.S. security experts warn that AQI is "weakened almost to the point of outright defeat in Iraq," but "remains lethal and has the potential to revive."[25] Because of violent incidents occurring in northern-central Iraq resembling typical AQI attacks, U.S. and coalition forces continue to conduct offensive measures against AQI leadership and strongholds to further weaken the group.[26] Experts believe that a significant number of AQI members are relocating to Pakistan to join AQ affiliates there.[27] Thus, AQI still poses a threat to U.S. interests.

Tehrik-e-Taliban Pakistan (TTP)

TTP is an AQ ally in the Federally Administered Tribal Areas (FATA) in Northwest Pakistan. Formed in 2007, TTP is an alliance of militant groups seeking to impose their version of *shari'a* law in Pakistan and to rid Afghanistan of coalition troops. Though distinct, TTP maintains "close ties to senior al-Qa'ida leaders, providing critical support to al-Qa'ida in the FATA and sharing some of the same global violent extremist goals."[28] Since 2008, TTP has repeatedly threatened to attack the United States. In fact, the failed 2010 Times Square bombing was executed by U.S. citizen, Faisal Shahzad,

[23] Katzman, Kenneth. *Al Qaeda in Iraq: Assessment and Outside Link* . Congressional Research Service, 15 Aug. 2008. Web. 31 Mar. 2011. <http://www.fas.org/sgp/crs/terror/RL32217.pdf>.
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.

who received training and financial support from TTP. In addition to this attack, TTP is also responsible for the April 2010 attacks against the U.S. Consulate in Peshawar, Pakistan, and for the suicide bombing in Khowst, Afghanistan, that killed seven Americans.

Haqqani Network and Harakat-ul Jihad Islami (HUJI)

Both Haqqani Network and HUJI are based in Pakistan, have close ties to AQ, and are intent upon attacking U.S. targets and persons in the region. Though these groups have yet to execute an attack in the West, they have the capabilities to do so. The Haqqani Network claimed responsibility for the 2008 attack against a hotel in Kabul that killed six, and has organized and participated in attacks in Afghanistan against U.S. and coalition troops.[29] In 2009, HUJI attacked Pakistani intelligence and police facilities in Lahore, Pakistan, killing 23 people.[30] Then, in 2007, the group attacked a mosque in Hyderabad, India, killing 16 people.[31] The lethality of these attacks demonstrates the groups' potential to inflict mass-causalities in the future, perhaps even in the West or against Western targets abroad.

Lashkar-e-Tayyiba (LT)

LT is a Sunni extremist group based in Pakistan which poses a significant threat to U.S. interests in South Asia. LT attacks in Kashmir and India "have had a destabilizing

[29] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[30] Ibid.
[31] Ibid.

effect on the region," by escalating tensions between New Delhi and Islamabad.[32] The most significant LT attack occurred in 2008 when the group launched eight simultaneous attacks in Mumbai, India focusing on civilian-centric targets including a hotel, a theatre, a tourist attraction, a college, and a café, that resulted in mass causalities and has become the paradigm of soft-target assaults. LT continues to plan attacks that could harm U.S. interests or citizens and to support AQ and the Taliban in Afghanistan in an effort to ouster U.S. and Coalition troops from that region.

Hezbollah

Hezbollah has operated continuously for more than a quarter of a century, during which time, the organization has developed capabilities "about which AQ can only dream, including large quantities of missiles and highly sophisticated explosives, uniformly well-trained operatives, an exceptionally well-disciplined military force of 30,000 fighters, and extraordinary political influence."[33] Hezbollah is both an army and a political party, and has gained control in Lebanon. Though Hezbollah has never attacked the United States, it is developing a presence in South America, particularly in the tri-border area between Brazil, Argentina, and Paraguay.[34] In 1992, Hezbollah claimed responsibility for bombing the Israeli embassy in Buenos Aires, an attack that killed 29 people. Then in 1994, Hezbollah bombed a Jewish community center in Buenos Aires, killing 85 people. Importantly, Hezbollah's patron is Iran, which is currently cultivating a

[32] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[33] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.
[34] Ibid.

strategic partnership with Venezuela. With Iran as its benefactor, many security experts warn that Hezbollah "would likely consider attacks on U.S. interests, to include the homeland, if it perceived a direct threat from the United States to itself or to Iran."[35]

"Homegrown" Terrorism

It would be disingenuous to discuss the threat of terrorism to U.S. homeland security without addressing the issue of domestic, or "homegrown," terrorism. In the immediate aftermath of 9/11, before the threat of terrorism had been fully conceptualized, rhetorical distinctions of "us," meaning Americans, versus "them," meaning terrorist, defined the U.S. narrative on terrorism. "Othering" the enemy creates a false distinction. As the terrorist events of 2009-10 convey, there is no impermeable line differentiating U.S. citizens from terrorists. Since 2009, "at least 63 American citizens have been charged or convicted of terrorism or related crimes."[36] In her written testimony submitted to the Senate Committee on Homeland Security and Governmental Affairs, Janet Napolitano, secretary of DHS, defined "homegrown" terrorists as: "terrorist operatives who are U.S. persons, and who were radicalized in the United States and learned terrorist tactics either here or in training camps in places such as the Federally Administered Tribal Areas of Pakistan."[37] Terrorist groups recruit U.S. citizens because of their knowledge of Western culture, American security practices, and the English language—skills that assist terrorist organizations in planning and executing successful attacks.

---

[35] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[36] Ibid.
[37] Ibid.

Though individuals radicalize for various reasons, the recent "spike" in homegrown terrorism is at least partially attributable to AQ propaganda with "a U.S.-specific narrative that motivates individuals to violence."[38] This narrative is disseminated over the Internet on English-language websites, and is best described as "a blend of [al-Qaeda] inspiration, perceived victimization, and glorification of past plotting."[39] Though it is unclear whether the recent increase in homegrown terrorist activity is truly a new development, as opposed to the mobilization of previously radicalized citizens, it is clear that AQ efforts to recruit U.S. citizens has intensified.

After the Fort Hood shootings in 2009, AQ public messages began advocating lone-operative attacks by U.S. citizens, while simultaneously deploring U.S. outreach to Muslim communities. AQAP also released *Inspire* magazine, an English-language online magazine that incorporates tips for "bomb-making, traveling overseas, email encryption, and a list of individuals to assassinate."[40] Online magazines, YouTube videos, chat rooms, and Websites provide English-speakers with access to terrorist networks. The result: an obvious increase in the mobilization of U.S. nationals who have been radicalized within the United States, and are intent on attacking America.

Methods of Terrorism

The calculus of risk assessment must include not only actors, but also methodologies, or, in other words, the means terrorists have to achieve their desired ends.

---

[38] United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.
[39] Ibid.
[40] Ibid.

Weapons and modes of terrorism have various gradations of lethality and availability. Thus, terrorists' power, and the risk they create for the United States, is defined by their ability to deploy various weapons. The following analysis considers potential modes of terrorism to assess American vulnerability within the context of each method of potential attack.

Improvised Explosive Devices (IEDs)

Historically, IEDs have been the most often used method of terrorism. This is because IEDs are easy to construct from ubiquitously sold, inexpensive materials. IED attacks are also popular with terror groups because they involve minimum risk; it is difficult to detect a bomb maker who buys seemingly innocuous supplies sold commercially on the open market. Additionally, most terrorists are able to install remote detonation capability on a bomb, allowing them to control both the time and distance from the explosion, thus facilitating escape.

Bombs are also attractive because there are detailed, accurate instructions on how to make IEDs available on various public websites and in books. For example, Amazon.com currently sells at least two books known to have precise instructions on bomb making: *The Anarchists Cookbook* and *Home Workshop Explosives.* Because of the strategic advantages of IEDs— with respect to cost, detection, and escape— and the widespread availability of both materials and instructions to make explosive devices, the U.S. will continue to face IED attacks abroad and likely at home as well.

Suicide Bombings

The first major suicide bombing by a non-state actor occurred in Beirut in 1981, at the hands of the Iranian-backed Shia group, Al-Dawa. The attack killed 27 and wounded 100—a level of lethality that inspired other terrorist groups to incorporate suicide strikes. This method of terrorism is appealing because, like IEDs generally, suicide terrorism is inexpensive. However, unlike planted IEDs, suicide terrorism is more precise—the terrorist can infiltrate the target and detonate the IED at any moment. Additionally, suicide terrorism guarantees media coverage, both because of the psychological damage of suicide attacks, and also because such attacks usually produce a spectacle in the form of mass confusion, disruption, and causalities. After interviewing 250 militant Palestinians, Nasra Hassan wrote of suicide terrorism: "Apart from a willing young man, all that is needed are such items as nails, gunpowder, a battery, a light switch, a short cable, mercury (readily available from thermometers), acetone, and the cost of tailoring a belt wide enough to hold six or eight pockets of explosives. The most expensive item is transportation to a distant Israeli town. The total cost of a typical [suicide] operation is about a hundred dollars."[41]

Suicide terrorists also do not have to make escape plans or fear the loss of group secrets if operatives are arrested. This mode of terrorism kills "about four times as many people on average than any other type of terrorism."[42] Furthermore, suicide terrorists can operate alone, meaning that individual, "lone-wolf," operatives can undertake a suicide mission remotely, such as in America.

[41] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.
[42] Ibid.

Assassinations

Assassinating a prominent public figure is an attractive option for terrorists because the death of an important person is psychologically disturbing to the public, likely to draw major media coverage, and will result in political, religious or other disarray as the targeted public official will need to be replaced. For these reasons, an assassination can be a very effective method of terrorism despite the fact that only one person is typically killed. To execute a successful assassination, terrorists often use IEDs because, as noted earlier, bombings are more likely to allow terrorists to escape detection than the use of handguns or other weaponry. Nevertheless, terrorists have used firearms in the past to assassinate public figures from close range. For example, in 2002, two assassins killed Marco Biagi, an Italian government consulate, with a handgun as Biagi entered his home. Assassinations are a common way to harm a foreign nation without having to infiltrate that nation. Thus, U.S. efforts to bolster homeland security may have little effect on the ability of terrorists to assassinate prominent U.S. officials abroad.

Missile Attacks

Missile launchers are expensive and easily detectable, and thus risky for terrorist organizations to use. The cumbersome nature of the weapon makes an expedient departure from the attack difficult, even under the cover of darkness. With missile launchers, "Unless terrorists operate in a friendly environment, operate within failed or failing states, or have secured getaway routes, there's always the risk of being caught."[43] Thus, terrorists typically do not use this technology, with the single exception of

[43] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.

Hezbollah. That group has been known to launch missiles into Israel with few, if any, repercussions.

Aviation attacks, hijackings

Hijackings, though an effective means of terrorism when successful, are contingent upon inept security measures in airports and on the actual plane. For this reason, hijackings have decreased in frequency over time. After 9/11, commercial aviation implemented a number of security measures to deter potential hijackers. For example, the U.S. Transpiration Security Administration (TSA) has implemented a "layered" security approach at U.S. airports which includes the following programs: Visible Intermodal Prevention and Response, Travel Document Checker, Behavior Detection Officers, The Secure Flight Program, Federal Air Marshalls, Federal Flight Deck Officers, Employee Screening, and Checkpoint Screening Technology. [44] Each of these programs will be explored in greater detail in Chapter Two.

There are, however, two primary concerns creating risk for commercial aviation hijackings. First, there are no internationally enforced aviation security guidelines, resulting in a fragmented security system with unquestionable disparities between the many international airports. In an article, "The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response," Anthony Fainberg notes that:

> "Standard risk assessment and risk mitigation formalism indicate that, given equivalent consequences, one should generally try to reduce vulnerabilities where threats are higher. The apparent inaction of the TSA in regard to flights originating overseas appears to violate this principle. Threats to civil aviation are most likely greater overseas than they are in

[44] Fainberg, Anthony. "The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response." *Homeland Security Affairs: The Journal of the Naval Postgraduate School Center for Homeland Defense and Security.* 3 Mar. 2011. <http://www.hsaj.org/?article=5.1.5>

> the United States, but the vulnerabilities of U.S.-bound overseas flights to terrorist attacks are greater than threats to domestic flights, not less. This is because equivalent technical security measures applied to civil aviation in the United States are not required for the overseas, inbound flights."[45]

Though the United States' security officials have often commented on the need for international security regulation standards, there has not been any significant effort to implement standardization. U.S. policymakers have been reluctant to lobby the international community for security regulations because of concerns about violating the sovereignty of other nations.

The second risk-multiplier for commercial aviation hijacking is the general aversion to new security technologies demonstrated by the American public. For example, in 2010 TSA introduced "advanced imaging technology," also known as full-body scanners, in 78 airports nation-wide (as of December 23, 2010).[46] After some 486 of these devices were implemented, there was massive backlash from the general public and the media over the invasiveness of the new scanners.[47] Opponents of the technology are concerned that the images produced by the machines, which show an outline of the passenger's naked body, invade personal privacy, despite the fact that these images blur the passenger's face. Additionally, the technicians operating these machines are isolated in a separate room to ensure that there is no interaction between the image-viewers and passengers.

---

[45] Fainberg, Anthony. "The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response." *Homeland Security Affairs: The Journal of the Naval Postgraduate School Center for Homeland Defense and Security.* 3 Mar. 2011. <http://www.hsaj.org/?article=5.1.5>

[46] Gulliver. "Full-Body Scanners: Which American airports have the new full-body scanners?" *The Economist*. 23 Dec. 2010.

[47] Ibid.

Nonetheless, the intense resistance to these machines has jeopardized the incorporation of the 300 additional machines planned for 2011.[48] This situation demonstrates the tension between civil liberties and security that precludes the implementation of the most effective security measures. Without universal standards for aviation security, and in light of the constraints imposed by the American public, commercial aviation will likely remain vulnerable to terrorist attack.

Kidnappings

Kidnappings are complicated operations requiring extensive planning, quick-thinking during the actual seizure, a network of operatives to support the operation while the victim is being detained, and a secure base of operation from which the perpetrators can communicate demands. The 1991 kidnapping and subsequent murder of CIA station chief, William Buckley, and Marine Colonel William Higgins by Lebanese terrorists is a paradigm of this type of terrorism. AQ kidnappings are characteristically not negotiating situations; victims tend to be murdered as an overt warning to target nations. In the past, such murders have been accompanied by the release of graphic video messages including footage of the brutal murders. A now infamous instance of this type of attack occurred in 2002, when Wall Street Journal reporter, Daniel Pearl, was beheaded in Pakistan. As in the Pearl case, kidnappings can generate massive media coverage and produce graphic images that become iconic symbols of the terrorists' power.

[48] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.

Mass Disruption

The most common threat of mass disruption is an attack against U.S. energy systems or critical infrastructure, particularly energy grids and gas pipelines. The potential consequences of this type of attack were realized on August 14th, 2003, when an accidental breakdown of the electric power supply structure in part of the Midwest, Northeast, and in Canada affected 50 million people.[49] Because energy systems in the United States are mostly privatized, security is fragmented even within industries. The major vulnerabilities of the energy sector are the lack of industry standards to protect against attacks, especially cyber attacks, and the unnecessary risk created by the close proximity of certain critical infrastructure, particularly petroleum pipelines.

With respect to the lack of industry standards, there is growing concern that certain potentially lethal industries, such as chemical research facilities and pharmaceutical laboratories, do not have sufficient security measures both within the facility and pertaining to personnel hiring practices. As for the close proximity of critical infrastructure, the vulnerability of the Gulf Coast region of the United States is apparent given the volume of oil pipeline that runs through that area. Additionally, other critical infrastructure, such as nuclear facilities and energy grids, are easily located and thus vulnerable to attack. An attack against the U.S. energy sector has not yet occurred because such an attack is complicated, requiring in depth understanding of the U.S. oil, natural gas, and electric supply chains as well as the computer systems controlling those sectors. However, Kevin King defines the growing inadequacies in the U.S. energy security policy in his essay, "Redefining U.S. Energy Security in the Twenty-First

[49] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.

Century." According to King, America "is in a state of deepening energy insecurity," and "stability in the vital regions that serve the international petroleum and natural gas markets will not be enough, even if this is possible to achieve."[50] In short, the U.S. energy sector is vulnerable, yet has not been attacked, not because of security policy, but because an attack against it would require a high degree of sophistication and planning by a capable terrorist organization.

Mass Destruction

The threat of a chemical, biological, radiological, or nuclear (CBRN) attack is the foremost concern in counterterrorism policy. Galvanizing concerns relating to CBRN attacks, is the fact that, after the dissolution of the Soviet bloc, weapons of mass destruction may have been leaked to terrorist groups or belligerent nations. Even those who contend that the dispersal of loose CBRN weapons is unlikely admit that Soviet expertise on the creation and maintenance of such weapons has surely reached belligerent nations, if not terrorist groups. The term "CBRN" encompasses a wide variety of weaponry and technologies that warrant individual discussion since there is considerable variation within this category with respect to risk.

[50] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.

Chemical

The risk of chemical attack is really concentrated on three potential agents: Mustard Gas, Sarin, and VX.[51] Mustard Gas can be either a gas or a liquid which sometimes smells like conventional mustard—hence the name. The agent works by attacking the skin causing severe blisters. It is most lethal when inhaled; in such instances, the agent causes lung and organ damage, and may even damage DNA. As a result of inhalation, victims can develop cancer, and if pregnant, birth defects. The threat of a Mustard Gas attack is not as significant as the threat of chemical terrorism using other, more lethal chemical weapons, especially because "there is no known instance of terrorists using Mustard Gas as a weapon."[52]

Sarin, in either its liquid or gas form, is much more deadly than most other chemical agents. Sarin can be absorbed through the skin or inhaled, and will kill victims within minutes of initial contact. Sarin works by attacking the victim's nervous system, muscles and organs. The Japanese cult, Aum Shinrikyo, produced Sarin in the 1990s and used it in an attack on the Tokyo subway system that killed a dozen people and injured over a thousand riders.[53]

VX is the most lethal nerve gas ever created. This agent is absorbed through the skin and attacks the nervous system, killing victims shortly after contact. This agent is very difficult to produce, but Aum Shinrikyo produced traces of VX as early as the 1990s.[54] The cult attempted to use the agent in several assassinations, one of which was successful. Though the Aum Shinrikyo is cult by far the most advanced terrorist group in

[51] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.
[52] Ibid.
[53] Ibid.
[54] Ibid.

terms of developing and using chemical agents in attacks, it is possible that chemical weapons may be developed by other terrorist groups in the future and used against the United States.

Biological

In the weeks following the 9/11 terror attacks, several letters containing spores of a lethal bacteria were mailed to members of the media and politicians. The perpetrator was never identified. As demonstrated by these attacks, biological weapons are both a dangerous and realizable threat to the United States. There are four biological threats to consider: anthrax, smallpox, botulinum toxin, and ricin.[55]

Anthrax can infiltrate the body via inhalation, ingestion, and even through skin abrasions. If anthrax enters the lungs, most victims die if not treated immediately because the anthrax spores will lodge deep in the lungs. If anthrax is absorbed through the skin or ingested, the spores are less lethal. To produce anthrax, a terrorist must grow the bacteria, free-dry (lyophilization) it, mill it to a 1-to-5-micron particles ratio, and then treat it with an antistatic coating.[56] When properly produced, anthrax is colorless, odorless, and capable of floating freely, like a gas. If an attack is not detected, the first symptoms of infection are flu-like and start 36-48 hours after contact. Even with antibiotic treatment, the prognosis for those showing symptoms is very poor. There are also concerns that, even if an attack is detected, there may still be mass casualties since "the U.S. Strategic National Stockpile (SNS) of key medicines and supplies is capable of flying prophylactic and treatment doses to any major city within twelve hours, but distribution to millions of

[55] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[56] Ibid.

residents in less than two days is extremely unlikely."[57] There is also concern that, in the event of a terrorist attack, there would not be enough antibiotic treatments available on short notice, and given that the window of time to counteract the biological agents is less than two days, any shortage in treatments would likely be fatal.

The smallpox virus is the second biological threat to U.S. homeland security. Although the virus was declared eradicated more than thirty years ago, the United States and Russia are known to have stores of the smallpox virus.[58] Before eradication, the virus spread insatiably, killing millions of people every year.[59] Regardless of its lethality, terrorist groups are not likely to use the smallpox virus in an attack because it is so contagious; however, there is still a small possibility that "a financially strong terrorist organization with scientists in its ranks could perhaps acquire smallpox through unemployed experts in the field who once worked in the Soviet Union's biological weapons program."[60]

Botulinum toxin, the third potential biological weapon to consider, is the most poisonous biological agent known. It is estimated that, if properly dispersed in its most concentrated form, botulinum toxin could kill a billion people.[61] After exposure to the toxin in potent concentrations, victims will experience muscle paralysis and die shortly thereafter. The Aum Shinrikyo cult attempted to produce a biological weapon that

[57] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.

incorporated both anthrax and botulinum toxin, however the weapon proved unsuccessful in the 12 attacks in which the cult tried to use the weapon in Tokyo from 1990-1995.[62]

Finally, ricin is a protein toxin found in castor beans that is "two hundred times more potent than cyanide" if inhaled, ingested, or injected.[63] There is no known antidote for this toxin; victims will die. The threat of ricin, although small, is real: in 2003, British police found a small quantity of ricin in a building just outside of London. Seven Muslim extremists were arrested in connection with the finding.[64]

In Afghanistan, coalition forces found small amounts of ricin and anthrax in several AQ operation centers and, in 2003, with the arrest of Khalid Shaikh Mohammed, U.S. officials discovered that AQ was planning to manufacture anthrax to be used against the United States in a biological attack.[65] Although AQ's bioterrorist aspirations have not yet materialized, there have been a number of biological attacks in the past, including: (1) the 1995 sarin gas attack executed by Aum Shinrikyo in the Tokyo subway; (2) Aum Shinrikyo's 1995 attempt to aerosolize anthrax in a Tokyo neighborhood; (3) the 2002 attempt to release cyanide on the London subway; (4) the 2003 attempt to use ricin on the London subway; and (5) the 2004 AQ attempt to release a chemical agent in Amman.[66] Clearly, biological terrorism is a realizable and potentially deadly threat to U.S. homeland security.

The effectiveness of a biological attack is largely determined by three factors: first, the specific agent used; second, the environment in which the agent is disseminated;

---

[62] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid.

and third, the delivery and dissemination process used in the attack.[67] With respect to the first factor, the selection, production and processing procedures for biological agents are critically important to the effectiveness of any biological weapon. After the biological agent is selected, and it is determined that the selected strain is an effective disease-causing agent, then the biological agent is processed to become a biological weapon.[68] The agent must be weaponized for easy dispersal in the air to reach the greatest number of people possible. The wetness or dryness of the agent is paramount to the dispersal process: "As a rule, it is difficult to produce highly weaponized dry bioagent but easy to disperse such material, and easier to produce wet agent but difficult to aerosolize it for widespread dispersal."[69]

As for the second factor—the dispersal environment—environmental conditions often govern the success or failure of a biological attack. With the exception of anthrax, "sunlight can degrade the material, rain might literally dampen the impact, and high winds or those blowing in the wrong direction can prevent infection of those targeted."[70] Finally, the third factor, the nature of the delivery and dissemination processes, is important in general but especially for wet biological agents which require precise equipment for large-scale aerosolization. Importantly, small-scale aerosolization is not difficult. Even simple household items like a perfume bottle can aerosolize wet biological agents. It is only when large-scale dissemination is attempted that mechanization becomes complex.

---

[67] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[68] Ibid.
[69] Ibid.
[70] Ibid.

Agricultural terrorism is a subset within the subject of biological terrorism. To date, there has never been an instance of agricultural terrorism directed against the United States. However, one RAND Corporation study detailing biological terrorist threats warns: "While several scenarios are possible, attacks against the agricultural sector could well pose the most serious threat, given their ease of management and potential socio-economic fallout (both of which fit well with the general evolutionary dynamic of al Qaeda in the post 9/11 era.)"[71] Small- and medium-size food processing and packing plants are vulnerable to infiltration. Thousands of these plants exist in the U.S., most of which have disparate internal quality control, insufficient biosurveillance, and largely unscreened workforces.[72] For example, many plants have no, or very few, exit and entry controls. RAND notes: "This lack of concerted and uniform security has served to increase the possibility of orchestrating a toxic/bacterial food-borne attack, which even in a limited form could trigger widespread psychological angst and social panic."[73] Processed food is distributed from a plant within a few hours of production. Thus, in the event of a terrorist attack, tainted food would disappear into food distribution channels and not be readily apparent or recoverable.

Agricultural terrorism could also include an attack against the U.S. cattle industry. Such an attack "would also fit well with al Qaeda's general emphasis on delivering a crippling blow to the American economy."[74] If a terrorist group weaponized foot-and-month disease, for example, the result could be equivalent to a smallpox epidemic. The

[71] CHALK, PETER. *Hitting America's Soft Underbelly The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*. The Rand Corporation. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2004/RAND_MG135.pdf>.
[72] Ibid.
[73] Ibid.
[74] Ibid.

weaponization process for such a disease is not difficult or expensive. To introduce foot-and-mouth disease, a terrorist would simply have to inject a cow with a viral sample; the disease is so contagious, and the American livestock industry so concentrated, that a multi-focal outbreak would likely occur.[75] The economic effects of an attack like this would be catastrophic. According to the Department of Agriculture, an outbreak of foot-and-mouth disease within the American beef supply would cost the United States billions of dollars in lost exports and potential trade sanctions and could disrupt the international beef market for years.[76]

Radiological

Unlike bioterrorism which is considered a less significant threat to U.S. security because of the complexity of creating and distributing bioweapons, radiological terrorism using a "dirty bomb" is a far more significant threat. Dirty bombs are conventional explosive devices containing radiological material; once the bomb explodes, the radiological material is dispersed and will contaminate the surrounding area. The lethality of dirty bombs depends on several factors, most notably: the potency of the radiological material used, the weather conditions at the time of detonation, and the speed of emergency responders.[77]

Constructing a radiological weapon is not significantly more complicated than constructing a conventional bomb. The primary obstacle for any terrorist is acquiring the

[75] CHALK, PETER. *Hitting America's Soft Underbelly The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*. The Rand Corporation. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2004/RAND_MG135.pdf>.
[76] Ibid.
[77] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.

radiological material. Obtaining this material, however, may not be as difficult as policymakers would like: "there are a myriad of sources internal to the United States that could be used for this purpose, ranging from radiation equipment employed in medical facilities to U.S. research stations, commercial sites, and atomic waste storage tanks located at prominent nuclear facilities found at military installations (something particularly true of radiotherapy clinics), and at least some power plants have already been locus of accidental atomic releases."[78] Radiological material could also be imported from outside the U.S., as was the case in 2003 when an AQ operative, Adnan El Shukrijumah, was discovered attempting to import radioactive components from a research facility in Canada. Shukrijumah was planning to use the radioactive material in an attack targeting the United Sates in 2004.[79]

Even if a radiological attack did not result in human causalities, the consequences would still be severe. Depending on the quality of the device, the sophistication of the plan, and the conditions at the detonation site, a very large area, encompassing tens of thousands of square miles, could be contaminated beyond habitability and require demolition.[80] Ports and major cities are the most concerning potential targets of a radiological attack. A recent RAND study considers the effects of the 2002 lockdown of 29 ports along the western seaboard of the United States as a substantive equivalent to the ramifications of a potential radiological attack. In the 2002 incident, the port closures resulted from a labor dispute between unions and management and lasted for almost two weeks. As result, 200 ships carrying 300,000 containers were delayed, with the direct

[78] Chalk, Peter, et al. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*. *RAND Corporation*. Center for Terrorism Risk Management Policy. 3 Mar. 2011. http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf
[79] Ibid.
[80] Ibid.

cost estimated to be $467 million.[81] Comparisons, like the RAND study, estimating potential losses from radiological attacks may seem far-fetched, but the threat of radiological terrorism is not hypothetical. In 2003, U.S. officials arrested an American citizen, with links to AQ, planning a domestic attack using a uranium-enriched radiological device.

Nuclear

Atomic terrorism is nearly impossible because building a nuclear weapon requires a sophisticated, fixed laboratory facility in which to produce the necessary fissile material – namely, highly enriched uranium or plutonium. This facility would be conspicuous and easily discovered by U.S. intelligence networks. Perhaps the difficulty of hiding production facilities is what inspired both AQ and Aum Shinrikyo to try to buy highly enriched plutonium from sources in Russia and other members of the former Soviet bloc in their attempt to create atomic weapons.[82] Even if a terrorist group were to acquire the fissile material for a nuclear weapon, however, it would not be easy to store because nuclear weapons require constant maintenance to be viable. As with producing enriched uranium, storing nuclear weapons would be obvious. Nevertheless, it is more likely that a nuclear weapons facility could be maintained covertly if its sole purpose were maintenance, not production, of nuclear missiles.

[81] Chalk, Peter, et al. *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*. *RAND Corporation*. Center for Terrorism Risk Management Policy. 3 Mar. 2011. http://www.rand.org/pubs/monographs/2005/RAND_MG393.pdf

[82] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.

In addition to the scenario in which a terrorist group buys the fissile material to produce a nuclear weapon, there are three other possibilities: first, that a terrorist organization could buy Russian non-strategic nuclear weapons left over from the Soviet Union on the black market; second, that a terrorist group could steal a nuclear weapon from a storage facility; and third, that a terrorist organization could receive a nuclear weapon from a failed or failing state with a nuclear arsenal but which is unwilling to overtly attack the United States. There are several nations with nuclear arsenals and strong, anti-U.S. leanings—North Korea has had the capability to build nuclear weapons since 2004, and Iran either has the ability now, or will soon have the ability, to develop nuclear weapons.[83] There is an emerging black market for nuclear technologies, materials and knowledge generally. In 2004, it became apparent that "the Pakistani scientist, A.Q. Khan, probably provided information about gas-centrifuges used to produce weapons grade uranium and nuclear bomb designs to North Korea, Iraq, Iran, Libya, and Syria."[84] There is also growing concern among experts that Iran will become a "clandestine source of fissile material for terrorists," once its nuclear program is proven credible.[85] Though nuclear weapons are an unlikely threat, relative to radiological, biological or chemical weapons (as will be discussed in Chapters 2 and 3), they merit consideration and prevention as the consequences for a nuclear attack are much more devastating than any other possible attack.

[83] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[84] Ibid.
[85] Ibid.

Cyberterrorism

In *Homeland Security: Assessing the First Five Years*, former Secretary of Homeland Security, Michael Chertoff, distinguishes the threat of cyberterrorism – defined as "a large-scale cyber attack against shared information technology and cyber infrastructure, including the Internet," – as "one of the most complex and potentially consequential" challenges of the 21st Century.[86] Of particular concern are cyber attacks against U.S. energy systems and cyber attacks coinciding with other terrorist attacks to prevent expedient action by first-responders. U.S. intelligence indicates that at least Russia and China have the technological capacity to disrupt American information systems and to hack U.S. computer systems to collect intelligence and critical information.[87] Terrorist groups, including AQ and Hezbollah have expressed a desire to launch cyber attacks against the United States. And, in recent years, these groups have demonstrated an increasing sophistication and ability to pursue such cyber attacks. In fact, there is an emerging illicit cyber capabilities and services economy for those with the financial resources to participate.

The threat of cyberterrorism is by no means unfounded. In 2002, the FBI discovered an unauthorized pattern of surveillance of the Silicon Valley computer systems. In collaboration with experts from Lawrence Livermore National Laboratories, the FBI traced the initial pattern to broader trails of reconnaissance.[88] In the FBI forensic summary of the investigation, prepared for the U.S. Defense Department, it was revealed that the investigation yielded evidence of "multiple castings of sites" across the U.S.,

[86] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.
[87] Ibid.
[88] Ibid.

routed through telecommunication switches in Saudi Arabia, Indonesia, and Pakistan. The infiltrators "studied telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities."[89] A number of the probes lead experts to conclude that there were plans for conventional attacks on the United States which would use "a class of digital devices that allow remote control of services such as fire dispatch and of equipment, such as pipelines."[90] Reason for concern is exacerbated by the 2008 confiscation of AQ computer systems on which resided more information about such remote control devices.

Because the Internet, information technology networks, and communications infrastructure are not government-owned or operated, cybersecurity is unlike other threats to U.S. homeland security. Cybersecurity is not exclusively the federal government's responsibility, and federal authorities "would not want to force a burdensome and intrusive security regime on one of the most dynamic and reliable engines of the U.S. economy."[91] However, cybersecurity cannot be a strictly private sector responsibility either, as the benefits from, and the reliance on, cyber infrastructure are dispersed throughout a myriad of other industries and society as a whole creating risk and vulnerability for all users in the event of a cyber attack. Cybersecurity is also complicated by the multiplicity of entry points, the lack of a central node or database, and the fact that no one individual, corporation or industry operates all information technology infrastructure. The threat of cyberterrorism is emerging and constantly increasing in sophistication, scope and capable actors.

---

[89] Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.
[90] Ibid.
[91] Ibid.

Other Vulnerabilities

Transportation Systems

The U.S. transportation system is porous and difficult to defend because it encompasses rail, road, air, and sea transport routes with a vast network of terminals, or nodes. Since the transportation sector is inextricably linked to commerce and the nation's economic well-being, components of the transportation system are ideal targets for terrorism. Specifically, the transportation sector "accounts for over 10 percent of U.S. GDP and about 20 percent of a household's expenditures, and employs over fourteen million people."[92] Historically, attacks on the transportation system have been conventional, usually involving IEDs. However, vulnerabilities within the transportation sector are expanding with the incorporation of new technology, like telecommunications systems. New computer systems are paramount to most forms of travel today. The integration of new technology adds the risk of cyber attack to the already risk-laden field of transportation security. Potential targets for cyber terrorists include: highway traffic controls, train control centers, air traffic control systems, and seaports.

Another result of technological advances is that transportation networks have become increasingly integrated and interdependent. Within an intermodal system, connection nodes become more vulnerable to attack and also more important to the viability of the system as a whole. If one node is debilitated, the repercussions may affect multiple components of the transportation system, disrupting the entire system. Security within the various modes of transportations, and at each node, is piecemeal—each unit

[92] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.

has unique security regulations and procedures. This further complicates security in that each mode of transportation, and perhaps individual nodes within sectors of the transportation system, must coordinate to create a layered security approach to prevent holes in the system. In this way, "intermodalism greatly complicates security calculations, particularly when we continue to think of security purely within one mode at a time."[93]

After the 7/7 attacks in London, there has been international scrutiny of public transportation security. Unfortunately, the volume of light rail, bus, subway, inter-city rail and commuter rail ridership makes screening each passenger untenable. For example, in the United States, over ten million trips are taken each day on metro and commuter systems.[94] To address the apparent vulnerabilities in public transportation systems the Federal Transit Association conducted threat assessments for major transportation systems; sent technical assistance teams to help individual transit agencies develop and implement security programs; developed chemical detection systems; promoted training and regional collaboration; created a public awareness program; and distributed security guidelines to local agencies.[95] The effectiveness of these measures has yet to be established, but even if they are effective, transit authorities are still concerned by the lack of funding to harden transit systems. There is a considerable funding disparity within transportation systems; "in the first few years after 9/11, for example, the federal

[93] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[94] Ibid.
[95] Ibid.

government allocated a mere $250 million to mass transit, compared to $15 billion for commercial aviation."[96]

In addition to subway attacks, port and maritime attacks are also of particular concern for U.S. homeland security. To prevent an attack on a port, incoming cargo must be screened soon after entering the port. Port authorities have been the most out-spoken opponents of port screening because, they argue, aggressive security measures will slow down shipping speeds, thus undermining U.S. trade advantages and domestic and international commerce. Currently, cargo is driven through screeners after being unloaded onto land transportation. This screening process prevents an attack targeting the interior, but if terrorists plan to attack the port itself, such screening measures accomplish nothing. Even when screening technology detects suspicious devices or substances, port personnel are not trained to determine which substances constitute potentially lethal materials, or what quantities of those substances are acceptable.

Finally, U.S. homeland security is threatened by the disparity between port screening practices in the United States and in foreign countries. Take, for example, one GAO study which found that some "35% of potentially dangerous containers were not screened in foreign ports due to diplomatic considerations and inadequate staffing."[97] Thus, the lack of international screening standards for foreign cargo into the United States, in conjunction with inadequate domestic screening measures and training standards, make U.S. ports lucrative targets for terrorism.

Air cargo is also a potential target for terrorist attacks, implicating both commercial and strictly cargo planes. The air cargo system is vulnerable because of the

[96] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[97] Ibid.

lack of security protecting cargo access ramps; because cargo must make many stops at various transposition nodes with disparate security measures; and because not all cargo is screened before being loaded onto air cargo carriers.[98] In a 2005 RAND study ranking various terrorist threats from lowest to highest (1-100, respectively), airplane hijackings did not even make the list, while a "bomb in uninspected cargo" received a ranking of 100. The complete list and rankings are as follows: Insider plants a bomb: 100; Bomb in uninspected cargo: 100; Large truck bomb: 71; Luggage bomb: 45; Curbside car bomb: 33; Attack on terminal passenger areas: 26; Attack on airplane runway areas: 26; Shoulder fired missile: 13; Attack on control tower or utility plant: 12; Sniper attack: 8; and Mortar attack: 3.[99] As this list demonstrates, threats to the U.S. transportation system extend beyond commercial aviation and encompass potential rail, road, sea, and cargo attacks.

Energy Systems

The U.S. economy relies on a predominately hydrocarbon energy system. An energy system is "the integrated network of primary energy sources, fuel refinement and power generation processes, and infrastructure that distribute energy for residential, commercial, industrial, military, and transportation end use sectors."[100] An energy system is defined by its inputs, throughputs and outputs. Inputs are primary energy sources in their raw form, such as crude oil; throughputs are the conversion processes including chemical, electrical, nuclear, and thermal; and outputs are the useable energy sources,

[98] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[99] Ibid.
[100] Ibid.

like refined fuels and electricity, as well as waste byproducts, like pollution.[101] An interconnected, complex network of manpower and infrastructure is necessary to manage the energy system at each stage (inputs, throughputs, and outputs) to ensure the U.S. energy supply.

In essence, energy security can be defined as a nation's secure and affordable access to sufficient supplies of primary energy. The U.S. energy system is vulnerable because of "its highly centralized and rigid networks, hazardous materials/fuel intensity, the lack of large-scale fuel substitutability," and the system's growing use of telecommunications networks and information sharing systems.[102] U.S. energy consumption is driven primarily by three sectors: petroleum, natural gas, and electricity, with coal and nuclear power representing a smaller share of U.S. energy demand. Each of these fuel sources contributes to satisfying U.S. energy demand, and thus any disruption to one of these sectors would impact the entire fuel supply chain and would be detrimental to the U.S. economy. Before considering the critical infrastructure facilitating the current U.S. energy system, which would be the likely target of future terrorist attack, it is helpful to first quantify American energy usage to contextualize the risk of damage to each component of the U.S. Energy system.

Petroleum

Petroleum satisfies 41% of U.S. fuel demand, the highest of any fuel source.[103] Approximately 90% of U.S. petroleum is converted into gasoline, while the remaining

[101] Terrorism and Homeland Security: Thinking Strategically About Policy. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[102] Ibid.
[103] Ibid.

10% is used as feedstock for the manufacture of plastics, chemicals, pharmaceuticals, foods, and other consumer products.[104] The U.S. economy literally runs on petroleum: "It is hard to think of many contemporary goods that are not produced from or do not utilize petroleum or its related products, in whole or in part, at some point in their development, transportation, or end use… Petroleum is not merely a commodity or fuel source, but the basis for a way of life."[105]

Notice, of the 21 million barrels of oil used in the U.S. everyday, 12 million are imported.[106] This creates additional risk since foreign oil dependence means that U.S. energy supply chains depend upon transportation security which, as previously discussed, is not secure. Another concerning facet of U.S. petroleum usage is that domestic demand is rising: the U.S. Energy Information Administration (EIA) models "indicate that petroleum demand will rise approximately 1.4% annually through 2025, when Americans will consume almost 28 million barrels of oil per day, 19 million of which will be imported."[107] Thus, American reliance on petroleum, in conjunction with the fact that large quantities of oil are necessarily imported, creates risk for U.S. homeland security.

Natural Gas

Natural gas satisfies 22% of the annual U.S. energy demand, with over 175 million users in the residential, commercial, and industrial sectors.[108] Natural gas is primarily used to heat and cool residential homes, and as chemical feedstock for the

[104] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.

production of other goods. In 2004, the United States used roughly 22 trillion cubic feet of natural gas, and yet produced only 18.7 trillion cubic feet. Thus, the U.S. imports 15% of its natural gas demand, mostly from Canada.[109] As with petroleum, the domestic demand for natural gas is forecast to increase through 2025: the EIA estimates that U.S. demand will reach 30.7 trillion cubic feet per year by 2025.[110]

Electricity

In 2004, more than 136 million users in the U.S. consumed more than 3,548 million megawatt hours of electricity.[111] The electricity sector is particularly vulnerable to terrorism because it is "characterized by a high degree of interdependency, meaning that a power loss in one aspect of the system can result in a cascading series of failures elsewhere."[112] To be clear, interdependency, in relation to the electricity sector, is defined as "the mutual functional reliance of essential services—on other networks, utilities, services, or auxiliary non-utility systems."[113] The physical interdependency of related services using electricity creates an endless list of possible threats since the loss of electricity would result in the loss of a range of dependent services from communications systems to the power supply. For example, with the loss of power comes the loss of first responders in the event of a terrorist incident. Other interdependencies exist because electricity is generated from other fuel sources including coal, natural gas, and nuclear power.

[109] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.

The economic repercussions of any large-scale loss of electricity are severe, as demonstrated by the August 2003 power failure in parts of the United States and Canada. In that instance, 50 million people lost electricity for days in the U.S. and weeks in Canada, and economic loss estimates from the event range from $4-$10 billion.[114] Even after power was restored, it took authorities months to determine the cause of the outage. The long investigation into the outage demonstrates the complexity of the current system in which "there are multitudes of opportunities for disruptions at the same time that there are lowering tolerances for disruptions."[115] More specifically, there are three major electric grids in the U.S.—the Eastern, the Western and the Texas Interconnections Systems—all of which connect into the Province of Quebec Interconnection.[116] To quantify the value of the U.S. electric grid, consider that the grid network has a generating capacity of over 960 gigawatts and is valued at over $1 trillion in assets.[117]

Coal

America has approximately 25% of the world's recoverable coal reserves, the highest of any country; and coal meets 23% of total U.S. primary energy demand.[118] At the present rate of use—about 1 billion short tons per year—the EIA forecasts that the United States has a coal supply of at least 250 years remaining.[119] Coal is cheap to produce making it an attractive fuel source for electricity-generating power plants: "coal-fired power plants account for approximately 92% of U.S. coal consumption and generate

[114] Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.
[115] Ibid.
[116] Ibid.
[117] Ibid.
[118] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[119] Ibid.

about half of U.S. electricity."[120] Despite a shift in energy policy to favor cleaner fuels, there will be 72 additional coal-fired power plants in operation by 2015.

Nuclear

Nuclear energy also helps to satisfy U.S. energy demand, providing about 20% of total electricity generation, or about 780 million hours of electricity, in 2004.[121] The tension that exists within the nuclear energy production sector is between the benefits of clean nuclear energy and the risk nuclear energy creates for both terrorism and public health. Nuclear power generation creates toxic nuclear waste that could potentially be used as a weapon or could harm the general public if not disposed of properly. There is momentum to convert to next-generation technologies, like pebble bed modular reactors which are smaller and generate less waste than traditional reactors, and are also "designed for safety, proliferation resistance, and ease of operation."[122] A large-scale transition to new technology requires time, but in the short-term, there is significant public opposition to constructing new conventional nuclear power facilities and, for this reason, nuclear power is not expected to increase its share of total U.S. energy consumption in the short-term.

Critical Infrastructure

The purpose of outlining the components of U.S. fuel demand is to demonstrate that energy security involves numerous sectors and an interdependent system. Critical

[120] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[121] Ibid.
[122] Ibid.

infrastructure is fundamental to the energy system, and is thus the likely target of any energy system terrorist attack. Crucial infrastructure, as defined by the National Strategy for Physical Protection of Critical Infrastructure and Key Assets, includes "facilities, systems and functions comprised of human assets and physical and cyber systems that work together in processes that are highly interdependent and reliant on key nodes for their operation."[123] To be classified as "critical," infrastructure must be important enough that its destruction would disrupt or foreclose crucial services at a national level, creating a threat to homeland security. In addition to critical infrastructure, there are individual targets whose destruction would cause mass casualties, significant property damage, or have a profound effect on national prestige. The common members of this class are nuclear power plants and dams.

The most vulnerable infrastructure systems, especially for petroleum (America's number one fuel source), are refineries and pipelines. These assets are susceptible to physical attack because they are stationary, conspicuously located, and largely consolidated in the Gulf Coast region. There is also the risk of cyber attack since many refineries and pipelines rely heavily on the Supervisory Control and Data Acquisition (SCADA) computer systems. Energy Sector nodes are particularly at risk: "a well-coordinated terrorist attack could take out the nation's gas transmission systems and keep key pipelines out of service for an extended period of time resulting in enormous personal and economic damage."[124]

The electricity sector is vulnerable to physical, cyber, and electromagnetic attacks. The threat of a physical attack on electricity systems is exacerbated by the highly

[123] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[124] Ibid.

centralized generation of U.S. electricity. Similarly, a cyber attack on the electricity system is also a concern because, like other Energy Sector components, the U.S. electricity system uses SCADA. Some experts refer to SCADA as "the Achilles' heel of the energy system," because of the heavy Energy Sector reliance on that network.[125]

In addition to this analysis of general threats facing U.S. energy systems, it is also necessary, in order to determine actual risk and security limitations for the U.S. Energy Sector, to quantify assets and infrastructure. To that end, consider the following figures: over two million miles of pipeline carry oil, natural gas, refined fuels, hydrogen, and other hazardous materials throughout the United States.[126] More specifically, 1.4 million miles of pipeline carry almost all of America's natural gas, and of this quantity, nearly two-thirds transverse public and commercial infrastructure at some point in transport.[127] There are roughly 700,000 active natural gas and oil wells in the U.S., as well as 2,000 petroleum storage terminals.[128] More than 17 million barrels of oil are refined each day in any of the 151 refineries nationwide; with 43% refined in facilities along the Gulf Coast, predominately in Louisiana and Texas.[129] Some 580 natural gas plants process over 60 billion cubic feet of natural gas per day, with more than 50% of that amount treated in facilities in Louisiana and Texas.[130] There are more than 3,000 independent utilities in the United States operating about 11,000 conventional coal, natural gas, petroleum, and duel-fire electric power plants.[131] American electricity is routed over 181,000 miles of high-

[125] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[126] Ibid.
[127] Ibid.
[128] Ibid.
[129] Ibid.
[130] Ibid.
[131] Ibid.

voltage power lines to commercial and residential destinations.[132] More than 65% of the nation's coal is at least partially transported by rail, and in some regions, there is only one railroad to deliver coal supplies.[133] Finally, as of 2005, there are 104 nuclear reactors in use, and another 36 research reactors located primarily at universities and other educational institutions.[134]

Energy security is encumbered not only by the size and complexity of the energy system, but also because no one agency or department is responsible for this sector of homeland security. There are a multitude of players involved in regulating and protecting the energy industry including: DHS, the Department of Commerce, the Department of Energy, the Environmental Protection Agency, the Department of the Interior, the Department of Transportation, the Federal Energy Regulatory Commission, the National Association of Regulatory Utility Commissioners, the North American Electric Reliability Council, and the Nuclear Regulatory Commission.

Furthermore, most critical energy infrastructure in the United States is privately owned, and most owners secure their assets only against low-level threats like vandalism and commercial espionage. This approach requires minimal effort and cost since less-than-perfect security is sufficient. For the private sector, the short-term gains resulting from minimal security outweigh the long-term benefits of more expensive security as terrorist attacks are a relatively small risk while profit is an immediate demand. To improve energy security, the government must intervene in markets to weight the cost-benefit analysis in favor of long-term security gains over individual profit. Each

[132] *Terrorism and Homeland Security: Thinking Strategically About Policy*. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.
[133] Ibid.
[134] Ibid.

proprietor's risk might be small, but an unprotected energy system creates an unacceptable aggregate vulnerability for homeland security.

This concludes the threat assessment for U.S. homeland security, but before considering homeland security measures and expenditures, it is helpful to contextualize risk by quantifying the threat posed by terrorism in the past as a model for current and future risk. The best way to do this is to examine trends in terrorism over time.

Trends in Terrorism: 1968-2009

This trend analysis uses the State Department's definition of a terrorist attack since the State Department is responsible for collecting and organizing terrorist attack data. To appreciate this trend analysis, it is crucial to understand the criteria used to determine what constitutes a terrorist attack. According to the State Department, "terrorism means premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, and is usually intended to influence an audience."[135] Most scholars of terrorism consider 1968 to be the first year in the modern era of terrorism characterized by more dramatic, large-scale events. The year 1968 is designated as "the significant breaking point" in the history of terrorism because, that year, Palestinian guerillas launched the first "sustained campaign of airline hijackings and sabotage… on a scale of violence and intensity never before seen by the international community."[136] Because 1968 is often cited as the beginning of modern terrorism, this essay will focus on attack data from 1968-2008. The year 2008 is

[135] "Office of the Coordinator for Counterterrorism." *The U.S. Department of State*. Web. 31 Mar. 2011. <http://www.state.gov/s/ct/index.htm>.
[136] LaFree, Gary, Sue-Ming Yang, and Martha Crenshaw. *Trajectories of Terrorism: Attack patterns of foreign groups that have targeted the United States, 1970–2004*. Stanford University, Web. 31 Mar. 2011. <http://iis-db.stanford.edu/pubs/22662/Crenshaw_Trajectories_of_terrorism.pdf>.

the last year considered in this analysis because 2008 is the last year for which there are completed annual terror incidents reports for both the State Department and the National Counterterrorism Center (NCTC).

The overarching trend to note for the last 20 years is that, while the number of terrorist incidents has decreased since 1990, the total number of causalities has increased significantly. From 1988-1992, there were 2,345 international terrorist incidents recorded resulting in 4,325 causalities (persons killed or injured).[137] Then, in the next five-year interval from 1993-1997, the number of incidents declined to 1,793 but with 13,092 casualties.[138] In the following five-year interval from 1998-2002, incidents again declined, this time to 1,649 and causalities rose once again to 16,807.[139]

Trend statistics change in 2003 and become incompatible with the pre-2003 method of classifying terrorist events. This is because, in 2003, the State Department chose not to count numerous terrorist incidents which distorted the figures to result in a decline in both incidents and casualties; this was subsequently revealed. In the revised report the numbers for both incidents and casualties showed marked increases from 2002. An investigation into the reporting discrepancy revealed that the State Department may have intentionally misconstrued data to claim that the U.S was making "significant progress in the war against terrorism."[140]

After this scandal, the State Department's "Patterns of Global Terrorism" report became the "Country Report on Terrorism." Thus, for 2004 and 2005, this paper

---

[137] LaFree, Gary, Sue-Ming Yang, and Martha Crenshaw. *Trajectories of Terrorism: Attack patterns of foreign groups that have targeted the United States, 1970–2004*. Stanford University, Web. 31 Mar. 2011. <http://iis-db.stanford.edu/pubs/22662/Crenshaw_Trajectories_of_terrorism.pdf>.
[138] Ibid.
[139] Ibid.
[140] Ibid.

employs the attack figures compiled by the NCTC which based their numbers on different criteria than the State Department. However, comparisons are again possible from 2005 onward because, beginning in that year, the NCTC collection methods included all terrorism incidents and were therefore compatible with the earlier State Department reports.

From 2005 through 2007, the number and lethality of terrorist incidents increased, but, interestingly, in 2008, there was an 18% decrease in number of terrorist incidents and a 30% decrease in the number of persons killed in terrorist attacks.[141] The table below represents the data from 2005-2008; figures are taken from NCTC.

Year	Number of Incidents	Number of Deaths
2005	11,156	14,616
2006	14,570	20,872
2007	14,499	22,685
2008	11,770	15,765

From 2005-2008, Iraq had more terrorist incidents than any other country. As a percentage of total terrorist attacks, Iraq represented 30% in 2005, 45% in 2006, and 43% in 2007.[142] In terms of total terror incident fatalities, Iraq represented 60% in 2005, 65% in 2006, and 60% in 2007.[143] In 2005-2008 the data overwhelmingly supports the notion that most terrorist incidents occur in the region in which the terror group is located. In those years, the Near East and South Asia had exponentially more incidents of terrorism

[141] LaFree, Gary, Sue-Ming Yang, and Martha Crenshaw. *Trajectories of Terrorism: Attack patterns of foreign groups that have targeted the United States, 1970–2004*. Stanford University, Web. 31 Mar. 2011. <http://iis-db.stanford.edu/pubs/22662/Crenshaw_Trajectories_of_terrorism.pdf>.
[142] Ibid.
[143] Ibid.

and fatalities than any other location. The table below depicts this trend and again, the figures are taken from NCTC.

	2005		2006		2007		2008	
	Attacks	Deaths	Attacks	Deaths	Attacks	Deaths	Attacks	Deaths
Near East	4,222	8,708	7,755	13,691	7,540	14,010	4,594	5,528
South Asia	4,022	3,046	3,654	3,609	3,807	4,737	4,354	5,826
East Asia/Pacific	1,005	758	1,036	854	1,429	1,119	978	762
Western Hemisphere	868	854	826	556	482	405	352	370
Europe/ Eurasia	780	373	659	220	606	227	774	292
Africa	256	879	422	1,643	835	2,187	718	2,987

As previously mentioned, the latest NCTC and State Department reports on terrorism look at incidents from 2008. According to the NCTC report, there were 11,800 attacks in 2008 resulting in over 54,000 deaths, injuries, and kidnappings.[144] Of those incidents, there were 235 high-casualty incidents (attacks resulting in 10 or more deaths), 75% of which occurred in the Near East and South Asia. In Africa, particularly in Somalia and the Democratic Republic of the Congo, the number of fatalities rose to 2,200, a 140% increase from 2007. Attacks in the Western Hemisphere decreased by 25% and attacks in East Asia and the Pacific declined by 30% from 2007 levels.

In 2008, according to NCTC, Muslims represented over 50% of the more than 50,000 victims of terrorist attacks; most of these deaths were a result of incidents in Iraq, Pakistan and Afghanistan. This finding is important because it indicates that terror groups may be making a tactical error by killing members of their base and thus undermining local support.

[144] *National Counterterrorism Center 2008 Report on Terrorism.* Web. 5 Apr. 2011. <http://www.fas.org/irp/threat/nctc2008.pdf>.

In the 2009 report, "Trajectories of Terrorism: Attack Patterns of Foreign Groups That Have Targeted the U.S., 1970-2004," Gary LaFree, Sue-Ming Yang, and Martha Crenshaw consider the 16,916 attacks executed between 1970 and 2004 by the 53 terror groups identified by the State Department as posing a significant threat to America. From that data, LaFree, Yang and Crenshaw determined that "just 3% of attacks by these designated anti-U.S. groups were actually directed at the U.S." and that "99% of attacks targeting the U.S. did not occur on U.S. soil but were aimed at U.S. targets in other countries."[145] Moreover, according to the study, 90% of attacks by these groups were domestic, occurring within the country in which the group is based.

The study also distinguishes two dichotomous trend lines between total attacks against the U.S and total fatalities resulting from those attacks. With respect to the first trend, total attacks, the series reveals that of the 111 total attacks against the U.S., the majority occurred in the mid-1970s and the early 1990s; in 1974 there were 38 attacks and in 1990 there were 41 attacks. After 1990, the number of total attacks declines until the end of the series (2004). Interestingly, the second trend line, total fatalities, shows that the number of total fatal attacks against the U.S. increased steadily in from the late 1990's until the end of the series in 2004. In fact, the peak year for fatal attacks occurred in 2004, the last year considered, with 9 fatal attacks. Notice, this series demonstrates that, though terrorist organizations are not attacking the United States with greater frequency, their attacks are becoming more sophisticated and deadlier.

Another important finding of this study is that terror groups that are considered a significant threat to U.S. security pose a more significant threat to other countries. For

[145] LaFree, Gary, Sue-Ming Yang, and Martha Crenshaw. *Trajectories of Terrorism: Attack patterns of foreign groups that have targeted the United States, 1970–2004*. Stanford University, Web. 31 Mar. 2011. <http://iis-db.stanford.edu/pubs/22662/Crenshaw_Trajectories_of_terrorism.pdf>.

example, in 1990, the peak year in the series for attacks against the U.S., there were only 41 attacks, whereas in 1991, the peak year of the series for non-U.S. attacks, there were 1,499 attacks. Likewise, there were 9 fatal attacks against the U.S. in the peak year of the series, 2004, whereas there were 536 fatal attacks against non-U.S. targets in the peak year of the series, 1989.

The Study also found that, of the 570 anti-U.S. attacks, only 5 (1%), occurred on U.S. soil. The other attacks, all occurring on foreign soil, included 233 attacks against U.S. businesses, 106 against diplomats and embassies, and 96 against the U.S. military. The remaining attacks struck various targets including educational institutions, journalists, nongovernmental organizations and tourists. These statistics indicate that proximity to the target is crucial in determining targets for terrorist attacks.

An analysis of trends in terrorism has several important implications for policymakers. First, anti-U.S. terrorist groups rarely attack the United States on U.S. soil, meaning that those responsible for allocating limited security funds must strive to protect U.S. assets abroad which are at greater risk of attack. Second, though the number of total attacks continues to decline, the lethality of those attacks has increased. This indicates that mass-causalities attacks are more prominent than in the past. Thus, security funds should be allocated to secure likely targets of mass-causality attacks.

This concludes the consideration of current risk to U.S. homeland security with respect to terrorist actors, weapons-technologies, attack methods and historical trends. The next chapter will address cost in terms of actual appropriations and existing threat-specific programs.

Chapter Two: Cost

The purpose of Chapter Two is: (1) to examine what Federal programs exist to address each of the threats to U.S. homeland security outlined in Chapter One; and (2) to determine how much money the Federal Government spends on these programs (and thus, how much the U.S. spends to address each threat listed in Chapter One). The threats outlined in Chapter One were: Foreign Terror Groups, Homegrown Terrorists, IEDs, Suicide Bombings, Assassinations, Missile Attacks, Aviation Attacks/Hijackings, Kidnappings, Mass Disruption Attacks (Critical Infrastructure Attacks), Mass Destruction Attacks (CBRN Attacks), Transportation Systems Attacks, Energy Systems Attacks and Cyberterrorism.

Funding comparisons for this chapter begin with fiscal year (FY) 2007 and end in FY 2010. This is because DHS underwent significant internal restructuring in 2006, making it difficult to compare current programs with those existing before 2007, and because, as of the writing of this paper, Congress has yet to pass a budget for FY2011. It is also important to acknowledge that the funding and programs recognized in this paper represent only programs whose *primary* purpose is to address the threat for which it is being cited. For example, there are several federal programs with information-gathering initiatives, but this paper only distinguishes intelligence programs with the sole purpose of gathering intelligence. This decision to focus on threat-specific programs has two implications. First, there may be other programs tangentially addressing the specific terrorist threats being discussed, but it would be disingenuous to include funding for those programs here since the purpose of this paper is to represent the true costs of U.S.

anti-terrorism efforts. And second, even though anti-terrorism is the primary mission of the programs distinguished here, a significant portion of their total program funding may go towards other goals. Program expenditures are not often outlined in detail, and thus it is usually impossible to determine the funding levels for initiatives within programs that deviate from the program's anti-terrorism mission. To return to an earlier example, initiatives within the National Intelligence Program (NIP) may address threats or missions unrelated to terrorism, but because intelligence programs are classified, there is no ability to differentiate true anti-terrorism funding from the aggregate whole. This paper attempts to deal with the issue of duplicitous program missions by selecting only programs whose primary mission is anti-terrorism; nonetheless, this system will not yield a perfect snapshot of U.S. anti-terrorism spending.

There are also negative externalities (such as reduced civil liberties) included in the cost considerations below. However, since such factors are unquantifiable, they are characterized as externalities (as opposed to a true cost). Even without a monetary value, these negative externalities are important because they are real—no one denies that increased intelligence authority to monitor U.S. citizens encroaches upon U.S. civil liberties. The debate over invasive security measures, therefore, is not about whether associated negative externalities exist in reality—they do— it is simply a question of whether one's liberty interest or one's security interest prevails with respect to each invasive program. This paper does not attempt to answer those normative questions, nor does it assign monetary value to negative externalities; not because doing so is a bad idea (in fact, that may be the most just way to factor unquantifiable rights into the policy cost-benefit analyses), but because doing so would extend beyond the scope of this project.

Instead, it is sufficient, for the purpose of this paper, to be aware of the negative externalities, and to consider them as having a generally negative value.

Limitations aside, this chapter will respond to each of the threats to U.S. homeland security outlined in Chapter One; some threats will be considered individually, and some will be considered in reasonable pairings with similar threats.

Intelligence: Countering the Threat of Foreign and Domestic Terrorists

The foundation of any effective counterterrorism strategy is intelligence. Without accurate intelligence, there is no ability to address *any* threat to U.S. homeland security—the government cannot counter risk if there is no intelligence to illuminate what threats exist. In Chapter One, there is an outline of the foreign terrorist organizations representing a significant threat to U.S. homeland security, as well as a discussion of the growing concern over "homegrown," or domestic, terrorism. For both foreign and domestic terrorism, intelligence is the necessary first phase of any defense strategy. Intelligence discovers which terror groups are plotting against the U.S., where those groups are currently located, what financial means the group possesses, the details of potential attacks, the leadership and internal structure of the group, and the ideological underpinnings and political motivations of group leadership. Without this information, the U.S. cannot defend itself.

Intelligence funding data, like the work of intelligence community members, is classified. Within the intelligence community, there are two distinct categories designated during the appropriations process: the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). NIP was formerly the National Foreign Intelligence

Program and the MIP includes all DOD and armed forces intelligence programs.[146] The NIP authorization legislation requires the Director of National Intelligence (DNI) to disclose aggregate annual funding levels for NIP; but there is no similar obligation for MIP officials. It is possible, therefore, to consider annual NIP funding levels, but it is not possible to differentiate program-specific funding levels, or even individual agency's funding levels, from the total NIP budget authority. The majority of NIP and MIP funding is housed in the Defense budget, but there are also intelligence funds in various other agency and department budgets including the State Department, the FBI and the DHS.[147]

The U.S. intelligence community includes: the CIA; the Bureau of Intelligence and Research, Department of State (INR); the Defense Intelligence Agency (DIA); the National Security Agency (NSA); the National Reconnaissance Office (NRO); the National Geospatial-Intelligence Agency (NGA); the Federal Bureau of Investigation (FBI); Army Intelligence; Navy Intelligence; Air Force Intelligence; Marine Corps Intelligence; the intelligence components of DHS; the Coast Guard; the Treasury Department; the Energy Department; and the Drug Enforcement Agency (DEA).[148] The CIA is the lead agency within the intelligence community because of its global sphere of operations that yield information on virtually every intelligence issue of interest for policymakers. Despite this prominence, it is the three DOD intelligence agencies— the NSA, the NRO, and the NGA—that consume the largest portion of intelligence funds.[149] The NSA is responsible for signals intelligence; the NRO manages reconnaissance

[146] Best, Richard A., Jr. *Intelligence Issues for Congress*. Congressional Research Service. 3 Mar. 2011. <http://www.fas.org/sgp/crs/intel/RL33539.pdf>.
[147] Ibid.
[148] Ibid.
[149] Ibid.

satellites; and the NGA collects geospatial data (meaning everything from physical maps to electronic databases) to help the military map areas in an armed conflict so that the U.S. can effectively use precision-guided weapons.[150]

For FY2010, NIP received $53.1 billion in federal funding; in FY2009, NIP received $49.8 billion in federal funds; and in FY2008, NIP received $47.5 billion in federal funds.[151] When indexed for inflation, the NIP funding levels for FY2010, FY2009, and FY2008 are $53.1billion, $50.6 billion, and $48.1 billion, respectively. Additionally, in a public appearance in September 2009, former Director of National Intelligence, Dennis Blair, said that the total annual intelligence funding, including both NIP and MIP, was $75 billion.[152]

NIP and MIP intelligence funding is used to facilitate four major intelligence collection systems, known as disciplines or "INTs."[153] The four major INTs are signals intelligence (*sigint),* imagery intelligence (*imint),* human intelligence (*humint),* and measurement and signatures analysis (*masint).*[154] Sigint is the analysis of foreign encryption systems; imint is the analysis of images from satellites, manned aircraft, and unmanned aerial vehicles (UAVs); humint is the collection of human intelligence, under both official and nonofficial cover; and masint is the application of complicated analytical refinements to information collected by signals and image intelligence operations.[155] A fifth, less significant, INT is open source information analysis (*osint*)

[150] Best, Richard A., Jr. *Intelligence Issues for Congress*. Congressional Research Service. 3 Mar. 2011. <http://www.fas.org/sgp/crs/intel/RL33539.pdf>.
[151] Ibid.
[152] Ibid.
[153] Ibid.
[154] Ibid.
[155] Ibid.

which is the study of publically available information like newspapers, books, radio, television and the Internet.[156]

As previously noted, intelligence gathering is perhaps the most important component of any counterterrorism strategy. Acquiring, analyzing and disseminating intelligence is critical to American security. There is, however, one unquantifiable and hugely important negative externality associated with intelligence: the violation of American citizens' privacy and civil liberties. The 9/11 attacks revealed the inability of national and international intelligence agencies to share information and to monitor U.S. citizens, leading lawmakers to pass the PATRIOT Act. This legislation is an unparalleled encroachment upon American civil liberties as it allows the federal government to monitor U.S. citizens in previously illegal ways. As this legislation demonstrates, there is a tension between the most sophisticated intelligence gathering capabilities and American civil liberties. To balance American security and liberty interests, it is necessary to take reductions in civil liberties into account as a cost of current intelligence initiatives.

First Responders: IEDs, Suicide Bombers, Missile Attacks and Mass Destruction

If efforts to counter terrorism fail, and the U.S. experiences an attack on American soil, first-responders are responsible for meeting the crisis and for beginning the recovery process. This is especially true of attacks involving IEDs, suicide bombers, missiles, and CBRN weapons, all of which are capable of causing mass destruction. The U.S. homeland security strategy is layered, not just in terms of multiple proactive efforts to counter terrorism, but also in that security officials recognize that a major component of

[156] Best, Richard A., Jr. *Intelligence Issues for Congress*. Congressional Research Service. 3 Mar. 2011. <http://www.fas.org/sgp/crs/intel/RL33539.pdf>.

mitigating the risk of an IED, suicide, missile or CBRN attack, is to strengthen the ability of first-responders to react to the attack. Because target selection is infinite, and because there are simply too many plots, actors, and means of attack to prevent every future terrorist incident, national investment in first-responders is the best way for the United States to directly address the risk and consequences of a successful terrorist attack using an explosive device.

Funding for emergency response teams comes primarily from state and local treasuries. The federal government augments first-responder funds to alleviate the burden of crisis planning for state and local budgets and to establish baseline standards for first-responder training, capabilities, and equipment. This examination of first-responder funding will only consider total federal funding, without regard for the specific segmentation and dissemination of federal funds to the various states, tribes, territories, and localities, because *federal* counterterrorism expenditures are the focus of this paper.

Federal funds for first responders come from the DHS budget, under the Federal Emergency Management Agency (FEMA) funding in *Title III: Protection, Preparedness, Response and Recovery.* Line items within this section for first-responders include "state and local programs," "firefighter assistance grants," "emergency management performance grants," "U.S. fire administration," "public health programs," "emergency food and shelter," and "management and administration" expenses.[157] Since counterterrorism expenditures are the focus of this paper—as opposed to total DHS expenditures—several line items of the FEMA budget were excluded from the funding totals represented below. All FEMA natural disaster response funding was removed

[157] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

because this paper considers only man-made disasters. Excluded line items include: "flood hazard mapping and risk analysis," "national flood insurance fund," "national flood mitigation fund," "national pre-disaster mitigation fund," and "the disaster assistance direct loan program."[158]

To address total U.S. expenditures on countering the threat presented by IED, suicide bombings and missile attacks (CBRN funds will not be including in this section, although first-responders do represent a key component of countering CBRN threats; instead, CBRN weapons will be subsequently addressed as an individual threat category), it is necessary to incorporate one other funding area within the DHS budget. *In Title IV: Research and Development, Training and Services*, under the "Science and Technology—Research, Development, Acquisition and Operations" funding, there is an "explosives" research line item.[159] When taken together, first-responder funding and explosives research funding for FY2010, FY2009, FY2008, and FY2007 totaled $12,178,670,000;[160] $12,408,594,000;[161] $11,781,550,000;[162] and $10,019,607,000,[163] respectively. When indexed for inflation, funding levels for the series become: $12,178,670,000 (FY2010); $12,746,272,930.85 (FY2009); $12,113,227,927.36 (FY2008); and $10,722,121,467 (FY2007).[164] First-Responder funding, therefore,

[158] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[159] Ibid.
[160] Ibid.
[161] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx
[162] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:
[163] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:
[164] Budget totals are indexed for inflation using annual CPI data.

decreased by 4.5% from FY2009 to FY2010, increased by 5.2% from FY2008 to FY2009, and increased by 13% from FY2007 to FY2008.

First-responders are responsible for assisting in incidents with various gradations of severity: some incidents can be handled at the local level; others classify as national disasters meriting federal intervention. Thus, the greatest challenge for first-responder units is to maintain the necessary level of preparedness to assist in worst-case scenarios even though day-to-day responsibilities are much less complex. In this way, first-responders split their time and resources between preparing for mundane incidents and preparing for unlikely, high-stakes events. To help first-responders manage this duplicitous objective, DHS created the *National Response Framework* in 2008 to clarify the operational response framework for all levels of authority. In addition to its governing function as the strategic architecture for incident first response, the *National Response Framework* also helps distinguish how federal first-responder funds are spent. Before discussing the ways in which federal funds are expended, it is useful to enumerate what actors comprise first-responder units at the local, state, and federal levels.

At the local level, first-responders include police, firefighters, emergency medical service providers, emergency management, public works, and environmental response professionals.[165] NGOs and not-for-profit organizations also constitute first-responders, since NGOs often perform critically important service missions (including providing food and shelter) and since there are a myriad of not-for-profit operators of critical infrastructure (particularly healthcare and power generation facilities) necessary for first-

[165] The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

responders to meet the demands of any crisis.[166] There are also local-level private-sector organizations which protect critical infrastructure facilities, networks, and communications systems, and thus also count as first-responders.[167]

State governments – and, more specifically, state governors—are responsible for organizing resources and coordinating response efforts with other jurisdictions including other states, First American tribes, and the federal government, if necessary. Disaster response resources available to states include state emergency management and homeland security agencies, state police, health agencies, transportation administrations, and incident management teams.[168] If state resources are insufficient to address a crisis, the governor can petition other states or the federal government for resource assistance through mutual aid agreements, such as the Emergency Management Assistance Compact.[169]

If the affected state's governor requests assistance, the federal government contributes to disaster and crisis response through a variety of programs and agencies that provide human, financial, and systems resources. There are also incidents that fall squarely under the purview of the federal government, namely those taking place on a military base, on a federal facility, or on federal lands.[170] After passage of the Homeland Security Act in 2002, the Secretary of Homeland Security became the official head of domestic incident management.[171]

---

[166]The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.
[167] Ibid.
[168] Ibid.
[169] Ibid.
[170] Ibid.
[171] Ibid.

The National Response Framework contains a "National Response Doctrine" that clarifies roles for first-responders at every level of government, and that constructs an operational framework to provide a layered incidence response that can be scaled to fit the needs of any crisis. "The National Response Doctrine" establishes five key principles: Engaged Partnerships; Tiered Response; Scalable, Flexible, and Adaptable Operational Capabilities; Unity of Effort Through Unified Command; and Readiness to Act.[172]

Engaged Partnerships mean that leaders from every level of government, in collaboration with private-sector, NGO, and not-for-profit partners, communicate to understand the goals, resources, and the role for each level of government within the national strategic framework. The most important aspect of the "engaged partnerships" principle is preparedness. According to DHS, preparedness is "the process of identifying the personnel, training, and equipment needed for a wide range of potential incidents, and developing jurisdictional-specific plans for delivering capabilities when needed."[173] To be prepared, partners from all levels of responders partake in training exercises and evaluation critiques to hone their response skills. These exercises are outlined in the *National Preparedness Guidelines* and the *National Exercise Program,* which contains 15 National Planning scenarios, focusing on 37 core capabilities that are the inspiration for a national exercise schedule.[174]

The second principle, "Tiered Response," simply refers to the DHS mandate that incidents are to be handled at the lowest possible level of government (or jurisdiction)

[172] The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.
[173] Ibid.
[174] Ibid.

and supported by additional resources and actors when necessary.[175] The third principle, "Scalable, Flexible, and Adaptable Operational Capabilities," refers to the DHS understanding that crises come in different sizes and have gradient scopes, complexities, and resource needs to which first-responders must be able to assess and then respond to meet the requirements of the specific incident, both initially and as response transitions to recovery.[176]

The fourth principle, "Unity of Effort Through Unified Command," is a detailed understanding of the chain of command that coordinates local, state, and federal efforts in a crisis. The Incident Command System (ICS) establishes a structure enabling agencies with divergent legal, jurisdictional, and functional responsibilities to harmonize their response efforts and resources.[177] "Readiness to Act," the fifth principle, refers to DHS' "forward-leaning posture" to engaging in incident response to prevent incidents from growing in size or complexity.[178] Implementing this principle requires nimble resources, human and otherwise, training exercises, incident communication and institutionalized response chains of command to allow resources to flow expeditiously to incident sites.

The final point to make about first-responder funding is that there are a host of other implicated federal departments and agencies whose budgets incorporate incident response funding, but which are not included in this paper. The reason these agencies and departments are excluded is because they do not actual *expend* federal funds for crisis response unless there is an incident, and this paper considers only actual spending, as opposed to total available funding.

---

[175] The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.
[176] Ibid.
[177] Ibid.
[178] Ibid.

Unlike DHS, which is involved in planning for crises, these other federal agencies engage in crisis management on a situational basis. DHS publishes a list of the situation-specific partnerships that support DHS efforts. To demonstrate this, consider the following list of possible targets and the corresponding agency or department that would then be involved in response efforts: (1) transportation systems: the Department of Transportation; (2) communications: the DHS; (3) public works and engineering: the DOD (U.S. Army Corps of Engineers); (4) massive fire: the Department of Agriculture (U.S. Forest Service); (5) public health epidemic: the Department of Health and Human Services; (6) oil and hazardous material spill: the EPA; (7) agricultural contamination: the Department of Agriculture; (8) energy systems: the Department of Energy; and (9) public safety or security concern: the Department of Justice.[179] As this list demonstrates, it would be disingenuous to present first-response as a DHS issue; depending on the nature of a crisis, there could be many involved agencies and thus funding for first-response could come from a number of various federal budgets. Again, because these funds are not expended annually, they are not considered here, and first-responder funding to counter the threat of a terrorist attack remains the exclusive product of DHS budget authority.

Before concluding this section of first-responder funding, it is necessary to discuss emergency communications systems. Especially after 9/11, DHS understands that a successful response to a terrorist attack – or any large-scale incident—requires a coordinated effort from first-responders comprised of representatives from public safety,

[179] The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>

public health, and the emergency management community.[180] The only way to organize these various first-responder units is with a functioning emergency communications system. To ensure state and local emergency communications systems are adequate, DHS provides funding to augment local budgets for the express purpose of strengthening emergency communications. In FY2010-FY2007, DHS provided $552,113,000 (FY2010);[181] $504,400,000 (FY2009);[182] $366,195,000 (FY2008);[183] and $251,114,000 (FY2007)[184] for the DHS Office of Emergency Preparedness Telecommunications and for the DHS Office of Emergency Communications. When indexed for inflation, the actual funding level for these DHS offices was: $552,113,000 (FY2010); $518,126,394 (FY2009); $376,504,238 (FY2008); and $268,720,600 (FY2007).[185] These figures demonstrate a 7% increase for emergency communications systems funding from FY2009 to FY2010; a 38% funding increase from FY2008 to FY2009; and a 40% funding increase from FY2007 to FY2008. This remarkable upward trend in DHS emergency communications system funding is part of a larger initiative to improve the emergency response weaknesses exposed by the 9/11 attacks.

[180] *National Emergency Communications Plan*. The Department of Homeland Security. Web. 14 Mar 2011. <http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf>.
[181] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[182] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx
[183] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:
[184] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:
[185] Inflation calculated using CPI data.

Assassination and Kidnapping

Assassination is a very common mode of terrorism, and is typically used to target politicians, diplomats, military personnel, dignitaries, and reporters. Kidnapping is a far less common means of attack, mostly because the logistics of executing a successful kidnapping are complex. However, kidnappings do occur, especially in failed or failing states. DHS relies on the U.S. Secret Service, an agency within DHS, to counter the threat to U.S. homeland security represented by assassinations and kidnappings of high-level political figures. The one caveat is that the Secret Service only protects civilians of significance. Thus, there are no preventative actions taken to avoid the assassination or kidnapping of mundane citizens, apart from basic information available to travelers on the State Department website. Once an average American citizen is killed or kidnapped, however, the U.S. does respond with force. This course of reactive (rather than proactive) action is the be strategy since a civilian assassination or kidnapping is not nearly as psychologically traumatizing to a population as the assassination or kidnapping of an important political figure. The magnitudes of those two terrorist scenarios (one involving an average civilian, the other a significant figure) are distinctly different, which is why is important to protect the powerful and socially important members of society, but not others.

U.S. Secret Service (USSS) funding comes from *Title II: Security, Enforcement, and Investigations* of the DHS budget, under the subheading: "U.S. Secret Service."[186] Funding levels for the USSS for FY2010-FY2007 were: $2,957,338,000 (FY2010);[187]

[186] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[187] Ibid.

$2,797,887,700 (FY2009);[188] $2,763,542,000 (FY2008);[189] and $2,545,866,000 (FY2007).[190] When indexed for inflation, these annual funding levels become: $2,957,338,000 (FY2010); $2,874,027,488.9 (FY2009); $2,841,342,109.7 (FY2008); and $2,724,366,783.1 (FY2007).[191] Thus, from FY2007 to FY2008, USSS funding increased by 4.29%; from FY2008 until FY2009, USSS funding increased by 1.15%; and from FY2009 to FY2010 USSS funding increased by 2.9%.

The USSS uses federal funding to fulfill its two-pronged mission "to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites and National Special Security Events (NSSEs)."[192] As the USSS mission statement explicitly notes, there are two key functions for Secret Service personnel: investigation and protection.

With respect to investigations, the USSS is responsible for protecting critical financial infrastructure by tracking and preventing the circulation of counterfeit U.S. currency, and by investigating financial and electronic crimes.[193] The proportion of counterfeit U.S. currency to genuine U.S. currency in circulation remains very low, only about .0001% of currency worldwide is counterfeit, but the total amount of currency in

[188] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx
[189] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:
[190] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:
[191] All numbers indexed for inflation using annual CPI data.
[192] United States Secret Service. *United States Secret Service Strategic Plan (FY2008- FY2013)*. U.S. Department of Homeland Security. Web. 6 Mar. 2011. <http://www.secretservice.gov/FY09_SecretService_Annual%20Report-Web.pdf>.
[193] Ibid.

circulation has grown steadily, doubling over the last decade, meaning that the sheer volume of fraudulent currency that exists has grown.[194]

Adding to USSS currency challenges are advances in technology, specifically printing and photographic computer technologies, which allow criminals to print fraudulent currency using over-the-counter inkjet printers.[195] Specifically, USSS determined that the level of digitally produced counterfeit U.S. currency increased from 1% to 54% over the last decade.[196] And while U.S. currency is redesigned every seven to ten years, older currency is left in circulation and thus fraudulent bills remain viable so long as the bill design after which the counterfeit piece is modeled is still accepted.[197] USSS efforts to combat counterfeit currency include: the use of fingerprint detection and forensic science in investigations; a continuous initiative to improve currency design, in collaboration with the U.S. Mint, the Department of the Treasury, and the Bureau of Engraving and Printing; studies of how U.S. currency circulates abroad; partnerships with private-sector actors to restrict the availability of commercial grade printers; and work with international financial institutions, governments, and law enforcement units to deter counterfeit currency originating abroad.[198]

As for financial crimes, advances in technology facilitated the proliferation of e-commerce, online transactions, and profoundly changed the nature of USSS investigations to include many more electronic crimes involving identity theft or a fraudulent payment system online. In 2006, e-commerce represented 2.74% of all retail

---

[194] United States Secret Service. *United States Secret Service Strategic Plan (FY2008- FY2013)*. U.S. Department of Homeland Security. Web. 6 Mar. 2011. <http://www.secretservice.gov/FY09_SecretService_Annual%20Report-Web.pdf>.
[195] Ibid.
[196] Ibid.
[197] Ibid.
[198] Ibid.

sales (about $100 billion), and, according to the Better Business Bureau, 8.9 million U.S. citizens were victims of identity theft, resulting in a loss of over $50 billion for victims and businesses.[199] USSS initiatives to investigate and prevent financial crimes include: efforts to prioritize investigations to focus resources on crimes with a "significant impact of the economy, the community and the critical financial infrastructure;" working with the financial payment industry to strengthen identification verification systems; and educating federal, state, local and international law enforcement agencies, as well as citizens and community leaders, on electronic and financial crime prevention and detection.[200]

The second prong of the USSS mission is to protect American leaders, visiting heads of state (and government), designated sites, and National Special Security Events (NSSEs).[201] Beginning in 1901, after the assassination of President McKinley, the USSS was charged with protecting the President of the United States. Shortly thereafter, that mission expanded to incorporate other national leaders, presidential candidates, visiting heads of state and government, some critical infrastructure, and events of national import.[202] Funds allocated for this mission go towards personnel needs, intelligence collection systems, new technologies and equipment, physical infrastructure security (such as the White House complex, the Vice President's residence, and foreign missions).[203]

---

[199] United States Secret Service. *United States Secret Service Strategic Plan (FY2008- FY2013)*. U.S. Department of Homeland Security. Web. 6 Mar. 2011. <http://www.secretservice.gov/FY09_SecretService_Annual%20Report-Web.pdf>.
[200] Ibid.
[201] Ibid.
[202] Ibid.
[203] Ibid.

The costs associated with protection of national leaders and certain pieces of significant national infrastructure extend beyond the USSS budget. There is also the unquantifiable cost with respect to access. Citizens of a democratic regime expect access to their elected officials. Unfortunately, the USSS efforts to protect national leaders severely limit public access to officials. Given the existence of terror plots, and assassination plots generally, it is not surprising that the USSS takes extreme precautionary measures to contrive the accessibly, and even visibility, of elected officials. This is a cost, however, and as a cost; limited access must be taken into account when examining the legitimacy of public expenditures to prevent assassination and kidnapping incidents.

Transportation Systems

The Transportation Security Administration (TSA) works with the law enforcement and intelligence communities to protect all components of the U.S. transportation system – including aviation, rail, transit, highway, and pipeline—to ensure the free movement of people and commerce.[204] Securing the entire transportation system is costly; fortunately, some of the funding burden for TSA is displaced through fee collections, the proceeds from which augment the TSA budget. After being indexed for inflation, but before the additional revenue from fees is taken into account, the net appropriation for the TSA in FY2010, FY2009, FY2008, and FY2007 was:

[204] *Transportation Security Administration*. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.

$5,258,446,000;[205] $4,400,558,200;[206] $4,133,875,570[207] and $3,816,967,062[208] respectively.[209] These figures indicate a 19.5% increase in congressionally allocated funds for TSA activities from FY2009 to FY2010; a 6.5% increase from FY2008 to FY2009; and an 8.3% increase from FY2007 to FY2008.

A true reading of the TSA budget, however, has to include all available TSA funds, which include the revenue from fee collections. After indexed for inflation, and once fees are taken into account, the TSA budget authority for series years FY2010-FY2007 was: $7,656,066,000 (FY2010);[210] $7,081,517,146 (FY2009);[211] $7,005,326,092 (FY2008)[212] and $6,755,608,117 (FY2007).[213] Thus, there was an 8% increase in total TSA budget authority from FY2009 to FY2010, a 1.1% increase from FY2008 to FY2009, and a 4% increase from FY2007 to FY2008.

TSA funds are used to support six program areas: grants, law enforcement, layers of U.S. aviation security, the Screening Partnership Program, the Transportation Systems Sector, and Reimbursement Agreements.[214] With respect to the first program area, the

---

[205] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

[206]Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx

[207] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:

[208] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:

[209] Inflation calculated using CPI data.

[210] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

[211] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx

[212] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:

[213] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:

[214] *Transportation Security Administration*. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.

TSA awards grant funding to help protect critical transportation infrastructure including transit systems, freight railroad carriers, ferries, and the trucking industry from acts of terrorism and other large-scale incidents.[215]

As for the second program area, there are four law enforcement programs funded by the TSA. First, the Federal Air Marshal Program –the primary law enforcement division of TSA—deploys federal air marshals on domestic and international flights to detect and respond to hostile acts committed during a flight targeting U.S. air carriers, airports, passengers and crews.[216] Second, the National Explosives Detection Canine Team uses highly trained dogs to locate and identify materials that may be dangerous to passengers or threaten the transportation system.[217] Third, Federal Flight Deck Officers are armed pilots who are authorized by TSA to use a firearm to respond to an act of criminal violence or "air piracy" to gain control of the aircraft.[218] Fourth, crewmembers are trained to serve a protective function through the Crew Member Self Defense Program, whereby flight and cabin crewmembers receive one-day, hands-on self-defense training, free of charge.[219]

The third TSA program area is the "layers" of U.S. aviation security, which include Visible Intermodal Prevention and Response (VIPR) teams, travel document checkers, behavior detection officers, the secure flight program, Federal Air Marshals, Federal Flight Deck Officers, employee screening, and checkpoint screening technology.[220] VIPR Teams support security efforts at critical transportation facilities in

[215] *Transportation Security Administration*. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.
[216] Ibid.
[217] Ibid.
[218] Ibid.
[219] Ibid.
[220] Ibid.

urban areas across the U.S., and are composed of Federal Air Marshals, Surface Transportation Security Inspectors, Transportation Security Officers, Behavior Detection Officers, and Explosive Detection Canine Teams.[221] Travel document checkers are Transportation Security Officers trained to use black light technology and magnifying loops to examine the identifications and boarding passes of passengers at every airport in the U.S.[222] Behavior Detection Officers use "non-intrusive" observation techniques to analyze the behavior of passengers to identify any potentially dangerous individuals.[223] The Secure Flight program is a TSA-operated watch list-matching program that services all airline carriers.[224] The Federal Air Marshal Program and the Federal Flight Deck Officer Program were defined above. TSA, through its Transportation Security Officer program, also screens airport employees working on the secure side of the airport— or the side that passengers reach after going through security.[225] The final layer of TSA aviation security is check point screening technologies, which are used to screen all baggage and passengers, and include: Imaging Technology (full-body scanners), Explosive Trace Detection, Explosive Detection System, CastScope (allows TSA to screen casts and prosthetics), Bottle Liquid Scanners, Threat Image Projection, and the Paperless Boarding Pass Pilot Program.[226]

The fourth TSA program area is the Screening Partnership Program (SPP or "Opt-out"), which allows airport operators to request to have security screening measures for their individual airport conducted by a private contractor working under federal

[221]Transportation Security Administration. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.
[222] Ibid.
[223] Ibid.
[224] Ibid.
[225] Ibid.
[226] Ibid.

oversight.[227] As of 2011, there are 16 U.S. airports making use of the SSP and private screening companies.[228]

The Transportation Systems Sector is the fifth program area funded by the TSA, and this sector encompasses all modes of transportation (aviation, maritime, mass transit, highway, freight rail, and pipeline), and is an interdependent, massive networked system.[229] The general security strategy for this system, as developed by the Office of Transportation Sector Network Management, calls for: (1) completion of industry threat, vulnerability, and consequence assessments; (2) development of baseline security standards; (3) assessment of operator security status versus existing standards; (4) development of a plan to close gaps in security standards; and (5) enhancement of systems security for each mode of transportation covered by the system.[230]

The Transportation Systems Sector is so vast that enumerating all of the roughly 120 programs within it would far exceed the scope and purpose of this paper.[231] To quantify the size of the Sector, consider statistics from a few of the Sector's component parts. With respect to freight rail, there are 559 railroads in the U.S.; 139,929 miles of track; 186,957 freight rail employees; 1,390,000 railcars; and the freight rail industry's annual revenue of $54 billion.[232] With respect to highway motorcars, there are 46,934 miles of interstate highway 116,813 miles of national highway system roads; 3,884,777 miles of other roads; 599,766 bridges (over 20 feet in span); 3,137 bus companies with 29,325 motor coach buses; and there are 703,000 active U.S. motor carrier companies

[227]Transportation Security Administration. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.
[228]Ibid.
[229]Ibid.
[230]Ibid.
[231]Ibid.
[232] Ibid.

operating nine million commercial trucks.[233] In addition, there are also 161,189 miles of hazardous liquid pipeline operated by over 200 operators; 309,000 miles of natural gas transmission pipelines; and 1,300 operators with 1.9 million miles of natural gas distribution pipelines.[234] Security programs within this sector address vulnerabilities within aviation, maritime, mass transit, highway, freight rail, and pipeline transportation systems.

The final TSA-funded program area is Reimbursable Agreements. The TSA Office of Acquisition, Reimbursable Agreements Team manages over 400 Other Transaction Agreements (OTA) awards, which are issued to U.S. airports "for the public good" and "to advance TSA security objectives" through the Law Enforcement Officer Reimbursement Agreement Program (LEO), the National Explosives Detection Canine Team Program (NEDCTP), and the Port Security Programs (PSP).[235] TSA uses risk, vulnerability, and consequence assessments as the primary way in which the agency attempts to allocate resources to industries and assets, but as demonstrated by the breadth of TSA initiatives, there are many unrelated modes of transportation comprising the larger interconnected network of the U.S. transportation system. TSA funds go towards programs to create nationwide transportation security standards and industry regulations in an attempt to secure this disparate and privately owned transportation networks.

[233] Transportation Security Administration. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.
[234] Ibid.
[235]Ibid.

Mass Disruption: Critical Infrastructure

The threat assessment in Chapter One describes a potential "mass disruption" attack as an assault against critical infrastructure. According to DHS, U.S. critical infrastructure include thousands of facilities that, if debilitated or destroyed, would cause mass casualties, significant economic loses, and/or threaten public health and the ability of the federal government to function.[236] Several communication networks and information sharing systems are also designated as critical infrastructure. The seminal text on critical infrastructure protection is the 2003 *National Strategy for The Physical Protection of Critical Infrastructure and Key Assets*. This report has been updated twice since publication, once in 2006 and again in 2009. The 2003 report created eleven critical infrastructure sectors and five key asset classes; the updated reports characterize the original key asset classes as independent sectors. This paper will use the original report categorizations, with eleven major sectors and five key asset classes, because this way of framing critical infrastructure demonstrates the funding priority given to the eleven major classes over the smaller asset classes housed within the larger sectors.

The original eleven sectors of critical infrastructure protection are: Agriculture and Food, Banking and Finance, Chemical, Communications, Defense Industrial Bases, Emergency Services, Energy, Healthcare and Public Health, Postal and Shipping, Transportation, and Water.[237] The five key assets classes are National Monuments and Icons, Nuclear Power Plants, Dams, Government Facilities, and Commercial Assets.[238]

---

[236] *CRITICAL INFRASTRUCTURE PROTECTION Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience.* United States Government Accountability Office. 1 Mar. 2011. <http://www.gao.gov/new.items/d10296.pdf>.

[237] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

[238] Ibid.

Although total funding for critical asset protection is an amalgamation of resources from federal, state, local, and private stakeholders, this paper will focus on DHS funds and efforts since DHS is the federal authority responsible for critical asset protection.

All funding levels in this section are derived from DHS appropriations legislation for the five-year period from FY 2006 through FY2010. In the last year of the series, FY 2010, DHS allocated $2,058,993,000 to critical infrastructure protection.[239] Before inflation is taken into account, the DHS funding levels for critical infrastructure protection for fiscal years 2007, 2008, and 2009 are $643,387,000;[240] $737,776,000;[241] and $1,004,167,000[242] respectively. When indexed for inflation, the absolute funding levels for 2007, 2008, and 2009 are $676,629,685.6; $747,206,242.7; $1,020,633,434 respectively. This means that funding levels for critical infrastructure trended upward for the four year period between 2007-2010 by 10.43% from 2007 to 2008, 36.6% from 2008 to 2009, and by 101.2% from 2009 to 2010. It is important to note that of that $2,058,993,000 allocated for DHS critical infrastructure protection in FY2010, $1,115,000,000 came from offsetting fee collections and thus is not a direct appropriation.[243] In no other year in the five-year series are offsetting fees included in critical infrastructure budget authority, and thus the cross-year comparison between FY2010 and all other series years shows a marked growth in critical infrastructure

[239] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[240] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. <http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:>
[241] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:>
[242] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx>
[243] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

funding for FY2010. If the offset funds (totaling $1,115,000,000) are excluded from cross-year comparisons, DHS critical infrastructure budget authority for FY2010 would have decreased by 7.51% from FY2009 (when indexed for inflation).

Total DHS spending levels for critical infrastructure protection are derived by combining investment totals from three areas of the DHS budget. Under *Title III: Protection, Preparedness, Response and Recovery*, there are three budget line items for critical infrastructure protection: the first two are under the subheading "National Protection Program Directorate" (these include spending for "Infrastructure Protection" and for the "Federal Protective Service"), and the third is under the subheading "Infrastructure Protection and Information Security."[244]

Now that funding levels for the series have been established, it is important to understand how critical infrastructure appropriations are spent. As noted above, there are eleven sectors of critical infrastructure to protect (Agriculture and Food, Banking and Finance, Chemical, Commercial facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Bases, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Information Technology, National Monuments, Nuclear, Postal and Shipping, Transportation, and Water), as well as, five key asset categories (National Monuments and Icons, Nuclear Power Plants, Dams, Government Facilities, and Commercial Assets). To give a nuanced account of critical infrastructure expenditures, each of these sectors and asset categories must be considered individually.

The first critical infrastructure sector is Agriculture and Food. In addition to DHS, the Department of Agriculture (USDA) and the Department of Health and Human

[244] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

Services (HHS) also play important roles in protecting the farms, food processing plants, laboratories, storage facilities, and transportation systems that comprise the assets in this sector of critical infrastructure protection.[245] According to *The Physical Protection of Critical Infrastructures and Key Assets* national strategy report, the Agriculture and Food sector includes the supply chains for feedstock, animals, animal products, seed and fertilizer; the crop production system; and the post-harvesting aspects of the food supply chain, such as processing, packaging, production, storage, distribution, retail sales, institutional food services, and restaurant/home consumption.[246] To quantify this sector, consider that it includes over 1,912,000 farms and 87,000 food-processing plants nationwide.[247]

Protecting critical assets in this sector involves countering the threat of intentional food contamination, perhaps from a biological agent introduced by terrorists, for a food and agriculture system that is decentralized, has many access points, and is largely privatized. Challenges to protecting agriculture and food systems in the U.S. are increasing as a greater percentage of American food is being imported, transported long distances, or extensively processed (either at home or abroad). To work to ensure food safety, the U.S. established a food-safety system to monitor critical control points in the agriculture and food supply chains with federal, state and local inspections of foodstuffs, food processing plants, food storage facilities, and food service establishments.[248] This system notwithstanding, protecting Agriculture and Food assets requires improved analytical methods for detecting biological agents in food products, in addition to

[245] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[246] Ibid.
[247] Ibid.
[248] Ibid.

enhanced laboratory capabilities. Current public health and agriculture laboratories are able to detect the presence of traditional human pathogens (unintentional contamination), but not unconventional agents (such as bio-agents that terrorists might use in an attack).[249]

Food and animal transportation is another area of concern within the Agriculture and Food sector. During long transportation routes, livestock, crops, and processed foodstuffs pass through various transportation hubs, are stored in interim facilities, and come into contact with a multitude of personnel and storage facilities. This has two implications for food safety: first, critical infrastructure protection must include the ability to impose standards for transporters, storage facilities and food/livestock handlers; and second, there must be a way to track the transportation of food and livestock to allow authorities to trace an outbreak back to the source of the contamination.

The final impediment to Agriculture and Food sector protection is the existing disincentive for information sharing and threat notification. Historically, in the event of contamination, individual producers (and, to a lesser extent, the entire market for the specific food product) pay the economic consequences for an outbreak. This means that if producers suspect serious contamination, they refrain from notifying authorities until it is certain because of the tremendous personal financial cost of contamination. The government must work to correct this market failure; in the event of a terrorist attack, it will be necessary to move quickly to counter the contamination which can only be done if the outbreak is reported expediently. The Agriculture and Food sector is an example of critical infrastructure that incorporates actual facilities – like farms and processing

[249] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

plants—as well as a large, decentralized system. It is import to begin thinking about critical infrastructure as more than individual buildings, monuments, and facilities.

The second critical infrastructure sector is Water. This sector is composed of two components: fresh water supply and wastewater collection and treatment. With respect to the first component (fresh water supply), critical infrastructure protection focuses on the 170,000 public water systems in the U.S. which depend on reservoirs (1,800 nation-wide), dams, wells, aquifers, pumping stations, aqueducts, and transmission pipelines.[250] Critical infrastructure protection for the second component (wastewater collection and treatment) focuses on the 19,500 municipal sanitary sewer systems, which includes 800,000 miles of sewer lines.[251] Wastewater facilities are responsible for collecting and treating sewage; for processing water from domestic, commercial, and industrial sources; and for operating storm water systems that collect and treat storm water runoff.[252]

To protect assets in the category, DHS, in partnership with the EPA, developed vulnerability testing for U.S. water systems and treatment facilities; has conducted threat assessments; and developed a secure information sharing system, The Water ISAC, to provide a forum for gathering, analyzing and sharing threat and security-related information among Water sector components. Because the Water sector encompasses so many assets, protection plans for this sector focus on attacks that would result in mass casualties, significant property damage, or major economic losses. More specifically, DHS distinguishes four concentration areas: (1) physical damage to, or destruction of, critical assets (including the release of toxic chemicals); (2) contamination of the water

[250] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[251] Ibid.
[252] Ibid.

supply; (3) cyber attack on ISAC, information management systems, or other electronic control systems; and (4) interruption of water services.[253]

Critical asset protection funds for this sector are also used to enhance facility capabilities to detect biological, chemical, or radiological contaminates in the water supply; and to address the risk created by inextricable interdependencies between water supply chains and other vulnerable sectors.[254] For example, the U.S. water supply is dependent upon a functioning energy sector— transporting water and wastewater requires pumps which run on electricity – as well as a functioning transportation system to carry chemicals required to treat water. Water supply systems also cannot function without telecommunication systems since water and wastewater treatment facilities are largely automated and controlled from remote locations.[255] Critical asset protection funds for this sector, therefore, are spent on hardening certain facilities, on contaminate detection systems, and on reducing the risk of system failure due to interdependencies with other vulnerable sectors.

The third sector is Public Health, which consists of state and local health departments, hospitals, health clinics, nursing homes, mental health facilities, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles.[256] To understand how truly massive the Public Health sector is, consider that it includes more than 5,800 registered hospitals.[257] DHS, with HHS, works to create resiliency in this sector since, in the event of a terrorist attack, functioning hospitals, clinics, and other

[253] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[254] Ibid.
[255] Ibid.
[256] Ibid.
[257] Ibid.

components of the public health system are required to treat attack victims. Even if a hospital is not the focus of a terrorist attack, if the chemical, biological, or radiological attack contaminates the area in which a major hospital is located, the effects of that attack could be catastrophic as there would be a debilitated capacity to treat victims.[258] Critical assets for this sector also include laboratories and facilities related to disease control and vaccine development and storage, such as the HHS Centers for Disease Control and Prevention, the National Institutes of Health, and the National Strategic Stockpile.[259]

Hospitals, and other publically accessible facilities in this sector, are difficult to protect because of the free-accessibility that corresponds with their function – by nature, hospitals let anyone in their front doors. There are varying degrees of security at U.S. hospitals; some are relatively secure while others are devoid of any security precautions whatsoever. Another concern is the variation in structural designs of American hospitals. Some hospitals are "immune-buildings," meaning that the actual building is constructed with design elements to prevent the spread of disease – such as controlled air flow systems, isolation rooms, and surfaces that eliminate infectious agents—while other buildings are not.[260] This creates vulnerability disparities within the sector that must be investigated using critical infrastructure funds.

Challenges with the maintenance, protection, and distribution systems for vaccine stockpiles and other critical emergency resources are also a drain on Public Health critical infrastructure funds.[261] There are two prongs to the issue of emergency resources: first, those resources must be maintained in a volume sufficient to address a potential

---

[258] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[259] Ibid.
[260] Ibid.
[261] Ibid.

terrorist attack; and second, emergency resources must be secured to avoid any potential contamination, tampering, or inadvertent harm that would compromise resource effectiveness.

With respect to the first prong, amassing the necessary volume of emergency resources is encumbered by legal and tax issues. The *Emergency Medical Treatment and Active Labor Act* mandates that hospitals treat any patient requiring emergency care, even if that patient does not have health insurance. In the event of a terrorist attack, hospitals would therefore be required to treat attack victims, regardless of their insurance status. However, once treatment is no longer classified as emergency care, the victim would be relocated to a non-emergency care facility, which is not legally required (or allowed) to treat patients without insurance. Thus, uninsured victims of a terrorist attack, if they did not have sufficient private means, would be sent back to critical hospitals, thereby overloading those facilities and compromising the ability of critical hospitals to provide emergency care to other attack victims.[262] With respect to the aforementioned tax issues, pharmaceutical companies are taxed on their product inventory creating a disincentive for vaccine suppliers to stockpile the amount of vaccines required to counter a major biological attack.[263] Thus, critical infrastructure funds for the Public Health sector are used not only to protect priority facilities, like specific hospitals that have critical capacities within their locality, but also to counter security disparities in the system and to correct market failures that deter the accumulation of an adequate stockpile of emergency resources.

[262] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[263] Ibid.

The fourth sector is Emergency Services, consisting of fire, rescue, emergency medical service (EMS), and law enforcement organizations from 87,000 U.S. localities which make up the first-line of response to any disaster or incident, both man-made and natural.[264] The 9/11 terrorist attacks exposed several weaknesses in this sector, including inadequate information sharing between agencies, telecommunications problems, and issues of inadequate force protection resulting from weak crime scene control and general inability to mitigate a second attack.[265] The most glaring issue, however, is the inability of multiple first-responder units, most notably police and fire units, to coordinate response efforts.[266]

Of great concern to critical infrastructure protection teams for the Emergency Services sector is the possibility of a terrorist attack that has two phases in which the first phase would draw first-responders to the attack scene, only to be the victims of the second phase of the attack.[267] Even if the second phase of this hypothetical attack was not calculated, there is still the inherent risk at any terrorist attack scene that first-responders will be contaminated by chemical, biological, or radiological agents in the atmosphere and thus create a second wave of victims. There is also the concern that no locality has a standing emergency response capacity to deal with the aftermath of a terrorist attack. Though mutual aid agreements make the flow of first-responders across jurisdictions possible, there would still likely be a shortage of first-responders in the event of another 9/11-scale terrorist attack.[268] Critical Infrastructure funds for this sector go towards

---

[264] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[265] Ibid.
[266] Ibid.
[267] Ibid.
[268] Ibid.

addressing this risk, along with the communication inadequacies mentioned above, coordination of planning efforts across jurisdictions and agencies, and efforts to protect first-responders at the scene of a terrorist attack.

The fifth sector is the Defense Industrial Base sector, for which DHS and the Department of Defense (DOD) oversee protection planning for at least 250,000 firms in 215 distinct industries.[269] The DOD relies upon private-sector contractors and industry to manufacture the majority of military equipment, supplies, materials, services, and weaponry used by U.S. armed forces domestically and abroad. To be efficient, DOD has a history of competitive bidding for contracts which, as a result of market forces for these competitive contracts, has reduced the number of redundant sources (and in some instances has eliminated all redundant sources entirely) for important military products and services. Redundant sources are often eliminated because U.S. military goods are highly specified and contracted services have unique and strict requirements. In other words, if a potential supplier of either goods or services fails to secure a military contract in a given year, that supplier will likely cease to exist because their only possible customer is the U.S. military. After that supplier goes out of business, the competitive bid process becomes less competitive since the pool of potential contractors has been diminished. This process repeats itself for several cycles until there is only one, or a few, suppliers of a specific good or service. Once redundant sources are eliminated, there are a relatively small number of private sector manufacturers whose individual security is inextricably linked to U.S. military strength.

[269] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.

In addition to protecting critical players in the U.S. armed forces supply chain, Defense Industrial Base sector critical infrastructure funds also go towards instituting and enforcing security standards for first, second, third, and fourth-tier subcontractors. DOD relies on outsourcing for both goods and services, but the competitive bidding process for military contracts does not take into account individual contractors' security protocols, and thus there are security disparities throughout the military supply chain. It is important to discover subcontractors with inadequate security practices to be sure that the U.S. military can operate without disruption in an emergency. To achieve this goal, Defense Industrial Base critical infrastructure funds go toward: (1) identifying critical installations and infrastructure; (2) creating site-specific protection plans for these designated nodes; (3) investigating subcontractors, and the military supply chain generally, to be sure that there are no security liabilities or unacceptable disparities; and (4) sharing information and threat assessments with private-sector contractors and manufacturers to be sure security corroborates with existing threats.

The sixth sector is Telecommunications. This sector is continuously evolving because of technological advances, business and market pressures, and changes in the regulatory environment. The telecommunications network includes both physical and cyber infrastructure. The "backbone" of the telecommunications network is the Public Switched Telecommunications Network (PSTN) which provides switched circuits for telephone, data, and leased point-to-point services for public and private users. PSTN is the largest physical infrastructure to secure, with over 20,000 switches, access tandems, and other pieces of equipment connected by nearly two billion miles of fiber and copper

cable. Mobile users are granted access to this wireless network via cellular, microwave, and satellite technologies.

The Internet and private enterprise networks are also critical pieces of infrastructure that have both a physical and cyber presence. Expansion in data network technology has created increased demand for Internet infrastructure to provide data services. Large Internet Service Providers (ISPs) grant access to public and private users through Network Operation Centers (NOCs) to manage high capacity networks. Small ISPs farm out their long-haul Internet traffic to larger ISPs and provide local Internet service via the PSTN. Both large and small ISPs connect to the PSTN through individual points of access—like a switch or a router—located in the main office of the specific Internet carrier. Even international Internet traffic is vulnerable since it employs underwater cables to transmit Internet activity to physical landing points in the United States. Enterprise networks are specialized networks that support the voice and data service needs of large corporation and enterprises. These networks use leased lines from the PSTN or Internet providers. When examined, all three of these components of the telecommunications system – the PSTN, the Internet, and enterprise networks—all combine physical and cyber infrastructure to create risk for DHS in the event of a terrorist attack.

The events of 9/11 demonstrated that even when they are not the predominate target of a terrorist attack, telecommunications networks can still suffer considerable damage, prevent first response efforts, and have lingering consequences for the U.S. economy. To prevent human or economic loss from disruptions to the telecommunications network, DHS uses critical infrastructure protection funds for the

Telecommunications sector to identify critical assets, harden those assets, and create contingency plans in case a terrorist attack occurs. Additionally, funds are used to create redundancies within the telecommunication network to prevent a shutdown and to create alternative routing pathways for communications. As with other sectors, Telecommunications is a largely private sector. This means that security costs for individual providers may outweigh any benefit those providers gain from increased security since the probability of being the targeted node in a Telecommunications attack is very small. It is the federal government's responsibility, therefore, to mandate certain infrastructure protections, and in most cases fund those protections, since individual vulnerabilities within the system aggregate to create an unacceptable level of risk for homeland security.

The seventh sector is Energy which DHS, in collaboration with the Department of Energy (DOE), divides into two segments: electricity and oil/natural gas. The electricity industry is comprised of over 2,800 power plants serving almost 130 million households and institutions.[270] Oil and Natural gas assets consist of more than 300,000 producing sites, 4,000 off-shore platforms, 600 natural gas processing plants, 153 refineries, 1,400 product terminals, 7,500 bulk stations, and 2 million miles of pipeline spanning the entire United States.[271]

Any disruption to U.S. electricity supply chains, particularly the destruction of a power grid, would prohibit activities that are crucial to the success of the U.S. economy and the ability of the nation to defined itself. The North American electric system is a multi-nodal distribution system with several interconnected nodes that supply almost all

[270] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[271] Ibid.

of the electricity to the United States, Canada and a significant section of Baja California Norte, Mexico.[272] The physical infrastructure of this system consists of generation, transmission/distribution, and control communications.[273] In addition to protecting specific nodes, DHS also requires system redundancies, back-up systems, and work-arounds within the system that would allow electricity providers to circumvent a damaged portion of the system in the event of a terrorist attack.[274]

Other critical infrastructure expenditures for electricity systems include DHS efforts to establish guidelines defining the necessary equipment to operate electricity networks. Once those guidelines are established, DHS works to stockpile critical equipment and to create restoration and recovery plans for the U.S. electric system. DHS is also working with federal, state, and local authorities to create mutual aid plans to prevent any one locality from being without electricity, and to implement redundancies in the system to prevent electric failure. Finally, DHS is working with private and public sector suppliers to establish standard risk assessment models and security protocols to ensure that critical assets are protected and that there are no security vulnerabilities from inadequate facility security, maintenance or personnel training.[275]

The second division within Energy critical infrastructure is oil and natural gas, two largely interconnected industries. The oil infrastructure consists of five components: oil production, crude oil transport, refining, product transport and distribution, and control/external support systems.[276] Natural gas and oil production include exploration,

---

[272] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[273] Ibid.
[274] Ibid.
[275] Ibid.
[276] Ibid.

field development, on –shore and offshore production, and field collection systems.[277] The transportation system for crude oil includes 160,000 miles of pipeline, storage terminals, seaports, and container ships.[278] Additionally, there are about 150 crude oil refineries with a variety of production capabilities ranging from 5,000 to over 500,000 barrels per day.[279] Finally, distribution of oil requires an extensive network of pipelines, trains, ships, ports, terminals, storage, trucks, and retail oil stations.[280]

The production processes for natural gas mirrors that of the oil industry, and is broken down into three major components: exploration/production, transmission, and local distribution.[281] Natural gas distribution in the U.S. utilizes a significant amount of infrastructure including storage facilities, gas processing plants, liquid natural gas facilities, and 270,000 miles of natural gas pipeline and 1,119,000 miles of natural gas distribution lines.[282] Citygates are nodes in the natural gas pipeline that connect the greater distribution system with local distribution systems to allow efficient natural gas distribution to a wide range of users nationwide.[283]

DHS and DOE critical infrastructure funds are used to create industry standards for electricity, oil, and natural gas production and distribution systems. The purpose of security standards is to create redundancy and resilience within each of these energy sectors to withstand any supply disruption resulting from an act of terrorist.[284] More specifically, DHS Energy sector initiatives for critical infrastructure protection include

[277] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[278] Ibid.
[279] Ibid.
[280] Ibid.
[281] Ibid.
[282] Ibid.
[283] Ibid.
[284] Ibid.

investments in research and development to enhance industry robustness for oil and natural gas; strategic planning efforts with state, local and private stakeholders to identify and counteract vulnerabilities in the energy supply chain; and efforts to coordinate equipment sharing plans to keep the supply chain functioning if a node is taken out or debilitated by an attack.[285]

The eighth critical infrastructure sector is Transportation which consists of several modes of transportation including aviation (there are over 5,000 public airports), maritime (300 coastal/inland ports), rail (there are 120,000 miles of major railroads in the U.S.), pipeline, highways (including 590,000 highway bridges), trucking/busing, and mass transit (500 major urban public transit operators).[286] U.S. transportation systems pose two significant problems for DHS efforts to protect critical infrastructure: first, the system is vast and encompasses an array of nodes, modes of transport, and locations nationwide; and second, the system is both internally and externally interdependent. Internal interdependencies exist because each mode of transportation is incapable of handling the entire volume of public transportation needs, and thus requires other modes of transportation to be viable; and external interdependencies exist because every sector of the economy depends upon a working transportation system.

DHS aviation critical infrastructure funds are used to identify the most vulnerable assets, including telecommunication networks and airport facilities; to identify threats to passengers; to improve security at points of access; to improve cargo-screening capabilities; and to research and develop new detection technologies.[287] For passenger

[285] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[286] Ibid.
[287] Ibid.

rail and railroad systems, DHS spends critical asset protection funds to improve shipment practices for hazardous materials, to develop passenger baggage and intermodal container screening capabilities, to develop a comprehensive modal risk assessment, and to create an information sharing system for all surface transportation components to relate cyber and physical infrastructure threats specific to railways or rail cargo.[288]

DHS plans to use highway, trucking, and busing critical infrastructure funds to: (1) execute a comprehensive risk assessment for these modes of surface transportation, (2) develop criteria for distinguishing and mitigating national and regional chokepoints, (3) make technology investments to harden critical facilities against acts of terrorism, and (4) create and implement a transportation operator education and awareness program for transportation security.[289] DHS critical Infrastructure protection initiatives for U.S. pipeline include a collaborative effort with the DOE and the Department of Transportation (DOT) to identify pipeline authorities and procedures to reconstitute facilities after any disruption from terrorism or otherwise; as well as an effort to identify system vulnerabilities, improve security plans, execute initiatives to deter specific threats, upgrade response plans, and address system interdependencies.[290]

Maritime transportation critical infrastructure funds are used for risk assessment, identifying best practices and vulnerabilities, developing implementation plans for new or responsorial security measures, coordinating international cooperation, developing port security, instituting security guidelines and security technologies for cargo and passenger

[288] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[289] Ibid.
[290] Ibid.

ships, and improving waterway security.[291] Mass transit critical infrastructure protection initiatives include creating security standards, managing interdependencies with other modes of transportation, and assessing existing impediments to enhanced security efforts, including legal, legislative, and statutory regimes.[292]

The ninth sector of critical infrastructure protection is Banking and Finance, for which DHS and the Department of the Treasury must prioritize protection for over 26,000 FDIC insured institutions.[293] Physical Banking and Finance sector infrastructure include buildings, human capital, and financial utilities, which house banking operations, financial markets, regulatory bodies, and the repositories for documents, records and financial assets.[294] DHS and Treasury funds for critical infrastructure protection are used to identify and combat the financial sector's dependency on telecommunications networks and information sharing systems, and to enhance information sharing capabilities to allow sector components to relate and share sector-specific threat and security information.[295]

The tenth sector is Chemical Industrial Hazardous Materials, which is overseen by DHS and the EPA, and consists of 66,000 chemical plants.[296] These plants produce an array of chemical products that are essential to other sectors, most notably health care, and which are often exported to international trading partners. Examples of goods produced by this sector are fertilizer for agriculture, chlorine for water purification, and

[291] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[292] Ibid.
[293] Ibid.
[294] Ibid.
[295] Ibid.
[296] Ibid.

the polymers used to create plastic from petroleum.[297] DHS and EPA funds for critical infrastructure protection for this sector are used to enhance site security and security standardization, to review legislation dictating the sale of toxic chemicals, and to continue to develop a sector-specific information sharing system to convey security information to component parts of this sector.[298]

The eleventh sector is Postal and Shipping which incorporates tens of thousands of postal facilities, hundreds of thousands of official drop-box locations, and 137 million delivery sites managed by more than 749,000 full-time United States Postal Service (USPS) employees.[299] USPS and DHS have identified several initiatives to be addressed by critical infrastructure funds, including improving mail and USPS facility protection capabilities, working to ensure the security of international mail, enhancing the USPS security information sharing system, conducting risk assessments for important facilities, and improving the ability of USPS to verify that the identity of the intended mail recipient and the identity of the customer receiving the mail item match.[300]

In addition to the eleven major critical infrastructure sectors, there are also five key asset classes: National Monuments and Icons (5,800 historic buildings), Nuclear Power Plants (104 commercial nuclear power plants), Dams (80,000 dams), Government Facilities (9,000 government owned/operated facilities protected by 1,225 full-time employees), and Commercial Assets (commercial centers, office buildings, stadiums, theme parks, and over 460 skyscrapers).[301] Components of these asset classes

---

[297] The Department of Homeland Security. *The Physical Protection of Critical Infrastructures and Key Assets*. 1 Mar. 2011. <http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf>.
[298] Ibid.
[299] Ibid.
[300] Ibid.
[301] Ibid.

exist within the constructs of the larger 18 sectors, and therefore there is no need to identify DHS protection initiatives for the asset classes, it is enough to note these asset classes are distinguished as critical.

Examining the architecture of DHS critical infrastructure protection demonstrates that there is a coherent plan prioritizing critical infrastructure by categorizing assets into sectors with specific strategic initiatives. This indicates that critical infrastructure funds are allocated purposefully and as a reflection of what policymakers determine to be the most important American assets. The critique of this strategy, however, is that it is inefficient to allocate limited security resources to harden assets and to protect components of important industries when there are infinite potential terrorist targets. Supporters of critical infrastructure protection cite the tremendous economic, political, and social import of protected assets as the justification for using resources to protect them. Supporters acknowledge that there are infinite targets, but argue that if an asset designated as critical were to be destroyed in an attack, the consequences of that loss far outweigh the cost of protection.

Opponents of critical infrastructure protection argue that it is legitimate to harden a small number of invaluable targets (such as the White House), but that the majority of critical infrastructure assets are essentially interchangeable, and for that reason, when one asset is hardened, any terror plot against that target will adapt to focus on a different, similar target. Thus, large-scale critical infrastructure protection is futile. Critical infrastructure protection is an example of an aspect of the U.S. homeland security strategy for which it is impossible to determine effectiveness—there is no way to know if there would be more terrorist attacks if targets were more susceptible.

There are also two negative externalities associated with critical infrastructure protection. First, when assets are classified as critical they become subject to increased security measures that limit public access to facilities with poignant national significance. The second implicit cost of critical infrastructure protection is the loss of privatization and free market forces. Several private industry sectors are designated as critical, and yet the federal government determined that security in those sectors was inadequate, even though there were market forces to dictate the security strategies adopted by individual stakeholders. Government intervention in private markets weights the cost-benefit analysis for individual stakeholders and moves the U.S. economy as a whole away from truly free markets and towards a social system. Like reduction in access, loss of free market principles is another implicit cost of critical infrastructure protection that is often discounted in legislation considerations because it is unquantifiable. These two negative externalities create cost for industry producers, and perhaps consumers as well, and thus should be considered in policymaking decisions.

Mass Destruction: Chemical, Biological, Radiological, and Nuclear Weapons (CBRN)

Although Chapter One details specific chemical and biological weapons, as well as the various radiological and nuclear threats, federal programs to counter these risks fall into the four major threat categories (chemical, biological, radiological and nuclear) without differentiating specific threats. For example, without a security clearance, there is no way to know how much money the U.S. spends to counter the threat of a Mustard Gas attack. This section, therefore, considers CBRN weapons programs without regard for the proportion of funding allocated to address specific threats within those general categories.

It is also worth noting that two previous sections of this chapter –intelligence and first-responder programs— are directly applicable to this section. The intelligence community helps to detect plots involving CBRN weapons, as well as discovers CBRN acquisition attempts domestically and abroad; and first-responders will be deployed to the attack scene in the event of a CBRN incident.

There are a number of CBRN-specific programs; these programs are some of the most well funded security programs in the United States. Chemical and biological attack prevention programs are grouped together in the DHS budget, while radiological and nuclear attack prevention programs are not differentiated at all because a radiological attack – such as a dirty bomb explosion—requires nuclear material. Thus, any program to deter a nuclear weapons attack also deters radiological attacks.

As will be discussed in greater detail below, nuclear attack prevention programs are facilitated by a host of Federal departments and agencies, most notably DOD, DOE, DOS and DHS, and thus nuclear programs are funded by an amalgamation of resources from various budgets. Federal chemical and biological security initiatives, however, are funded exclusively by DHS. There are two sections of the DHS budget pertaining to chemical and biological weapons programs. First, in *Title III: Protection, Preparedness, Response and Recovery,* under the subheading "Office of Health and Affairs," there are several biological and chemical weapons-specific programs, including BioWatch, the National Biosurveillance Integration Center, and the Rapidly Deployable Chemical Detection System.[302] And second, in *Title IV: Research and Development, Training and Services,* under the subheading Science and Technology –Research, Development,

[302] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

Acquisition and Operations, there are two chemical and biological weapons-specific research line items: "Chemical and Biological," and "Laboratory Facilities."[303] When the two chemical/biological-specific spending categories are taken together, DHS investment to counter the threat of a chemical or biological attack in FY2007, FY2008, FY2009, and FY2010 was $270,032,000;[304] $291,479,000;[305] $410,978,000;[306] and $366,681,000[307] respectively. When indexed for inflation, actual spending levels for the series become: $288,965,061.7 (FY2007); $299,684,809.1 (FY2008); $422,162,072.2 (FY2009) and $366,681,000 (FY2010).[308] These figures indicate a 13.1% decrease in federal spending from FY 2009 to FY2010, a 40.9% increase in federal spending from FY2008-FY2009, and a 3% increase in federal spending from FY2007 to FY2008.

Though funded in consort, there are distinct programs to counter chemical versus biological attacks. With respect to chemical attacks, there are only two realizable scenarios: first, a terrorist organization could develop the scientific know-how to produce a lethal chemical agent in a laboratory, and then weaponize that agent for dispersal; and second, a terrorist organization could steal a lethal chemical agent from a laboratory without having to learn to produce the agent independently. The first scenario does not require (nor lend itself to) specialized programs to counter the threat of highly capable terrorist organizations because if such organizations exist – as they do in Japan—the only

[303] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[304] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:
[305] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:
[306] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx
[307] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[308] Inflation calculated using CPI data.

effective way to detect and deter plots is to use intelligence and surveillance to monitor the group's activities. The second scenario is far more likely than the first, mostly because developing chemical weapons is a sophisticated art that is unimaginable for almost all terrorist organizations. In other words, the only plausible track to for most terrorist groups to obtain chemical weapons is to steal them from a chemical facility, or to co-opt an employee of a chemical facility with access to developed chemical weapons.

In response to this second scenario, the DHS created statutorily enforced Chemical Facility Anti-Terrorism Standards (CFATS). As of the most recent data, collected in June of 2010, there are 4,997 facilities operating under CFATS, with facility locations in all fifty states.[309] The purpose of the CFATS initiative is to establish minimum security levels for chemical facilities so as to prevent external infiltration from outside actors, as well as internal resource leaks, both in terms of human capital (knowledge) and actual chemical material. To that end, CFATS incorporates vulnerability assessments, security plans, compliance reviews, personnel screening, and storage protocols. As of 2010, according to DHS data, there have been over 6,000 Security Vulnerability Assessments; over 38,000 Top-Screens; over 3,100 Site Security Plans; over 244 Compliance Assistance Visits at chemical facilities by DHS inspectors; and over 150 facility-specific outreach discussions.[310] Chemical facilities are privately owned and operated, which means that the most DHS can do to address the threat of chemical terrorism is to institute security regulations and verify through inspections that facilities meet those basic requirements.

---

[309] The Department of Homeland Security. *Update on Implementation of the Chemical Facility Anti-Terrorism Standards and Development of Ammonium Nitrate Regulations*. 2010 Chemical Sector Coordinating Council Security Summit. http://www.dhs.gov/xlibrary/assets/chemsec_summit_2010_cfats%20update_sue_armstrong.pdf

[310] Ibid.

As for biological weapons-specific homeland security measures, DHS has two biosurveillance systems—meaning early detection and warning systems—to counter the bioterrorist threat. These two programs, the National Biosurveillance Integration Center (NBIC) and BioWatch, are the only strictly biological terrorism prevention programs within the U.S. anti-terrorism programs arsenal.[311] NBIC is an information center created by the 9/11 Commission Act of 2007 to detect any biological events posing a national security risk for the United States.[312] The purpose of NBIC is to "rapidly identify, characterize, localize, and track a biological event of national concern; integrate and analyze data relating to human health, animal, plant, food, and environmental monitoring systems; and to disseminate alerts to member agencies, and state, local, and tribal governments."[313] NBIC is also responsible for operating the National Biosurveillance Integration System (NBIS), created in 2004, which is an IT system used to integrate data for surveillance of environmental, human, plant, and animal health, as well as biological agent intelligence and threat information.[314]

BioWatch, created in 2003 as a system to detect the presence of airborne biological agents, deploys detectors in 30 cities nationwide to manually collect air samples (using stationary filters) to be analyzed for biological agents on the BioWatch threat list. Once collected, BioWatch air samples are analyzed in state and local laboratories, and results usually take 10 to 34 hours from the time of the dangerous biological agents' detection. To expedite the analysis process, DHS is working to replace

---

[311] Jenkins, William O., Jr. *BIOSURVEILLANCE Preliminary Observations on Department of Homeland Security's Biosurveillance Initiatives. Government Accountability Office.* July 16, 2008. Web. 10 Mar. 2011. <http://www.gao.gov/new.items/d08960t.pdf>.
[312] Ibid.
[313] Ibid.
[314] Ibid.

existing detectors with Generation 3.0 detectors that would collect and simultaneously analyze air samples; DHS began implementing this technology in 2010.

In addition to chemical and biological attacks, the U.S. homeland security strategy also addresses the risk of a nuclear or radiological attack. Like chemical and biological terrorism, the best strategy to counter the risk of a nuclear or radiological attack is a robust intelligence program, and well-trained first responders to react to an attack if one occurred in the United States. There are, however, a number of nuclear and radiological weapons-specific programs to augment intelligence efforts.

As previously mentioned, there is no need to differentiate between nuclear and radiological weapons prevention since deterring both radiological and nuclear terrorism involves controlling nuclear materials. Thus, the Defense Department, the Nuclear Regulatory Commission (NRC), and the Department of Energy through the National Nuclear Security Administration (NNSA) are responsible for deterring a nuclear or radiological attack through domestic and international initiatives to control nuclear material and regulate nuclear facilities. Funding levels for each of these three components will be detailed in the subsequent program descriptions, but the aggregate spending levels (defined as the combination of total budget authority for all three) for nuclear and radiological defense programs for FY2010, FY2009, FY2008, and FY2007, when indexed for inflation, were: $30,040,540,000; $30,667,967,014; $22,129,504,247; and $22,007,967,311 respectively.[315] There was, therefore, a 2% funding decrease from

[315] Inflation calculated using CPI data. Pre-inflation adjusted numbers for NRC are from: The U.S. Nuclear Regulatory Commission. *Performance and Accountability Report — NRC Summary of Performance And Financial Information Fiscal Year 2010*. Web. 10 Mar. 2011. <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1542/v16/s1/sr1542v16s1.pdf>. Pre-inflation adjusted numbers for DOD are from: D'Agostino, Davi M. *Weapons of Mass Destruction: Actions Needed to Track Budget Execution for Counterproliferation Programs and Better Align Resources with Combating WMD Strategy*. Government Accountability Office, 28 Sept. 2010. Web. 10 Mar. 2011. <http://www.gao.gov/new.items/d10755r.pdf>.

FY2009 to FY2010, a 39% funding increase from FY2008 to FY2009, and a 0.55% funding increase from FY2007 to FY2008.

Beginning in 1975 as a product of the Energy Reorganization Act of 1974, the NRC became an independent federal agency responsible for regulating nuclear power plants; nuclear facilities; the transportation, storage and disposal of nuclear material and waste; and other civilian uses of nuclear products including medical programs, academic activities, research projects, and industrial uses.[316] NRC funding levels for FY2010, FY2009, FY2008, and FY2007 were: $1,066,900,000; $1,045,500,000; $926,100,000 and $824,900,000 respectively. When indexed for inflation, budget authority for the series become: $1,066,900,000 (FY2010); $1,073,951,516.9 (FY2009); $952,171,860.5 (FY2008) and $882,737,017.3 (FY2007).[317]

To accomplish its mission, NRC establishes and enforces standards and regulations and issues licenses to nuclear facilities and users. NRC regulations cover the entire nuclear power production process to ensure nuclear material is handled appropriately and that nuclear facilities meet basic security requirements. To understand the breadth of NRC's regulatory function, consider the complexity of the nuclear fuel production process: first, uranium is mined and then milled uranium ore is transformed

---

Pre-inflation adjusted numbers for NNSA are from the annual appropriations legislation available at: An Act Making Appropriations for Energy and Water Development and Related Agencies for the Fiscal Year Ending September 30, 2010, and for Other Purposes. PUBLIC LAW 111–85—OCT. 28, 2009. Web. 10 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ85/pdf/PLAW-111publ85.pdf>.H.R.1105—Omnibus Appropriations Act, 2009. *Thomas*: Library of Congress, Web. 10 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1105.enr:>.H.R.2764— Consolidated Appropriations Act, 2008. *Thomas*: Library of Congress, Web.10 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:>. Budget authority for DOE programs granted through a series of four continuing resolutions available online through the Library of Congress *Thomas* Website: "Status of Appropriations Legislation for Fiscal Year 2007." *Thomas*: Library of Congress.Web.10 Mar. 2011. <http://thomas.loc.gov/home/approp/app07.html>.

[316] The U.S. Nuclear Regulatory Commission. *Performance and Accountability Report — NRC Summary of Performance And Financial Information Fiscal Year 2010*. Web. 10 Mar. 2011. <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1542/v16/s1/sr1542v16s1.pdf>.

[317] Ibid.

into "yellow cake," a uranium concentrate.[318] The yellowcake is transported and converted into uranium hexafluoride gas and then transported to a gaseous diffusion plant and enriched into reactor fuel.[319] After uranium is fabricated into fuel pellets and loaded into metal rods, they are bundled into reactor fuel assemblies and transported to nuclear power plants (104 nationwide).[320] The process ends when nuclear waste and byproducts are transported from power plants and stored or disposed of.[321] To control access to nuclear material and the nuclear fuel production system, NRC has issued 3,000 licenses for nuclear materials users (as of 2011), and conducts roughly 1,200 inspections of license holders annually.[322] There are also 37 states, operating in partnership with NRC, with primary oversight jurisdiction over their jurisdiction's nuclear industry and some 19,600-license holders across their respective territories.[323] Thus, the primary function of NRC is to establish and enforce regulations, in collaboration with both users and states, to control nuclear energy production and usage in other sectors.

The DOD is involved in preventing a nuclear/radiological terrorist attack through the Counterproliferation Program Review Committee (CPRC) chaired by the Secretary of Defense. Though operated as a component of the DOD, other members of CPRC include the DOE, DOS, DHS, and the Office of the Director of National Intelligence. CPRC coordinates a multitude of counterproliferation programs for other federal agencies that prevent the acquisition and development of nuclear weapons. The diversity and volume of programs under CPRC jurisdiction is too great to detail in this paper; there are 228

[318] The U.S. Nuclear Regulatory Commission. *Performance and Accountability Report — NRC Summary of Performance And Financial Information Fiscal Year 2010*. Web. 10 Mar. 2011. <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1542/v16/s1/sr1542v16s1.pdf>.
[319] Ibid.
[320] Ibid.
[321] Ibid.
[322] Ibid.
[323] Ibid.

CPRC programs, 43 of which have at least two nuclear/radiological weapons-specific missions.[324] However, examples of CPRC programs include: developing a comprehensive strategy for the eight weapons of mass destruction mission areas (security cooperation and partnership activities, threat reduction cooperation, consequence management, interdiction, elimination, passive defense, active defense, and offensive operations); organizing, training, equipping, and preparing military forces to combat nuclear weapons delivery systems; and serving as the principle military advisor to the President and Secretary of Defense regarding combating nuclear weapons (a function the Chairman of the Joint Chiefs of Staff serves).[325]

CPRC has significant annual budget authority to coordinate its many programs. Funding levels for CPRC for FY2010, FY2009, FY2008, and FY2007 were: $19,100,000,000; $22,400,000,000; $14,300,000,000 and $14,400,000,000.[326] When indexed for inflation, CPRC budget authority for the series is: $19,100,000,000 (FY2010); $23,009,578,172 (FY2009); $14,702,578,129 (FY2008) and $15,409,641,229 (FY2007).[327]

The final component of the U.S. anti-nuclear/radiological weapons strategy is the NNSA, which operates under the DOE, to detect, secure and dispose of nuclear and radiological material.[328] More specifically, NNSA's threefold mission is to "detect nuclear and radiological materials, and WMD-related equipment; secure vulnerable

---

[324] The U.S. Nuclear Regulatory Commission. *Performance and Accountability Report — NRC Summary of Performance And Financial Information Fiscal Year 2010*. Web. 10 Mar. 2011. <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1542/v16/s1/sr1542v16s1.pdf>.

[325] D'Agostino, Davi M. *Weapons of Mass Destruction: Actions Needed to Track Budget Execution for Counterproliferation Programs and Better Align Resources with Combating WMD Strategy*. Government Accountability Office, 28 Sept. 2010. Web. 10 Mar. 2011. <http://www.gao.gov/new.items/d10755r.pdf>.

[326] Ibid.

[327] Inflation figures calculated using CPI data.

[328] *The National Nuclear Security Administration*. The U.S. Department of Energy, Mar. 2011. Web. 10 Mar. 2011. <http://nnsa.energy.gov/>.

nuclear weapons and weapons-useable nuclear and radiological materials; and dispose of surplus weapon-useable nuclear and radiological materials."[329] Detection programs include research and development efforts to improve nuclear detection technologies, work with international partners to interdict nuclear and radiological weapons trafficking, and training initiatives to educate export control and customs officials about WMD-awareness.[330] Initiatives to secure nuclear material and weapons include: security programs targeting Russia and former Soviet-bloc countries that potentially hold loose nuclear material or weapons; programs to convert research reactors to low enriched uranium (as opposed to highly enriched uranium); and efforts to strengthen international export regulations.[331] And, finally, examples of NNSA disposal efforts include programs to replace Russian heat and electricity generation systems so that Russia will stop producing weapons-grade plutonium as a byproduct of antiquated Russian nuclear reactors, and programs to dismantle and then dispose of nuclear material in excess U.S. warheads that are being dismantled.[332]

To accomplish this threefold mission, NNSA has an annual budget authority of $9,873,640,000 (FY2010);[333] $6,410,000,000 (FY2009);[334] $6,297,466,000 (FY2008)[335] and $6,275,583,000 (FY2007).[336] Once indexed for inflation, funding levels become:

---

[329] *The National Nuclear Security Administration*. The U.S. Department of Energy, Mar. 2011. Web. 10 Mar. 2011. <http://nnsa.energy.gov/>.
[330] Ibid.
[331] Ibid.
[332] Ibid.
[333] An Act Making Appropriations for Energy and Water Development and Related Agencies for the Fiscal Year Ending September 30, 2010, and for Other Purposes. PUBLIC LAW 111–85—OCT. 28, 2009. Web. 10 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ85/pdf/PLAW-111publ85.pdf>.
[334] H.R.1105—Omnibus Appropriations Act, 2009. *Thomas*: Library of Congress, Web. 10 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1105.enr:>.
[335] H.R.2764— Consolidated Appropriations Act, 2008. *Thomas*: Library of Congress, Web.10 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:>
[336] Budget authority for DOE programs granted through a series of four continuing resolutions available online through the Library of Congress *Thomas* Website: "Status of Appropriations Legislation for Fiscal

$9,873,640,000 (FY2010); $6,584,437,325 (FY2009); $6,474,754,257 (FY2008) and $6,715,589,065 (FY2007).[337]

Although DHS nuclear and radiological weapons-prevention programs are included under NNSA and CPRC jurisdiction, there is one nuclear/radiological line item in the DHS budget that is separate from NRC, CPRC, and NNSA efforts, but which was excluded from the aggregate nuclear/radiological funding total above. This program was not included before because it is a research and development program that is ambiguously defined and thus cannot be said to directly counter nuclear weapons. In *Title IV: Research and Development, Training and Services,* under Science and Technology – Research, Development, Acquisitions, and Operations there is a "Radiological and Nuclear" subheading with a series budget authority of: $150,188,000 (FY2010);[338] $161,940,000 (FY2009);[339] $103,814,000 (FY2008)[340] and $105,649,000 (FY2007).[341] When indexed for inflation, funding levels become: $150,188,000 (FY2010); $166,346,924 (FY2009); $106,736,605 (FY2008) and $113,056,471 (FY2007).[342] These figures indicate a 10% funding decrease from FY2009 to FY2010; a 56% funding increase from FY2008 to FY2009; and a 6% funding decrease from FY2007 to FY2008. This concludes the CBRN weapons-specific programs section of the costs associated with the U.S. homeland security strategy.

Year 2007." *Thomas*: Library of Congress.Web.10 Mar. 2011. <http://thomas.loc.gov/home/approp/app07.html>.

[337] Inflation calculated using CPI data.

[338] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

[339] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx

[340] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:

[341] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:

[342] Inflation calculated using CPI data.

Energy Security

Energy systems security is a sector within the National Infrastructure Protection Plan (NIPP), and thus, energy security efforts were outlined briefly above in the "Critical Infrastructure" section of this chapter. Although there is no additional energy-sector critical infrastructure funding to report here (beyond that which was included above), energy sector security efforts merit further inquiry since, as Chapter One indicates, a terrorist attack targeting the U.S. energy system would be devastating. With that in mind, this section will examine the Energy Sector security strategy as outlined by DOE in the Energy Sector-Specific Plan (SSP), an annex to the NIPP.

The purpose of energy security efforts is to create a "robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private partners at all levels of industry and government."[343] To achieve this vision, the Energy SSP lists six security goals: (1) establish secure, reliable, and timely information sharing systems; (2) enhance physical and cyber security measures based on sound risk assessment; (3) conduct comprehensive disaster, emergency, and continuity planning to prepare emergency response units; (4) define critical infrastructure protection responsibilities for public, private, state, local, and tribal partners; (5) understand and address energy

[343] United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*Web.13 Mar. 2011. < http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>

interdependencies; and (6) strengthen public confidence in the Energy Sector's resiliency and emergency/disaster preparedness.[344]

To be clear, the Energy Sector includes three major resource classes: electricity, petroleum, and natural gas; and each of these classes has its own set of infrastructure and activities to protect. To demonstrate the security challenge posed by the sheer size of the Energy Sector, consider the processing cycle for each of these three fuel sources. Before electricity can be used as a household fuel source, it must be generated (using fossil fuels like coal, natural gas or oil, or by using nuclear, hydroelectric, or renewable energy sources), it is then transported and distributed using substations, lines, and controls centers.[345] Before petroleum can be used as fuel, it must be mined as crude in onshore or offshore fields, held briefly in terminals from which it is transported using pipelines to processing facilities to be refined and transported, again using pipelines, to storage facilities, control systems, and petroleum market operators.[346] Finally, before natural gas is used as fuel, it must be mined from onshore or offshore fields, processed and then transported and distributed using pipelines to storage and liquid natural gas facilities, from which it can be transported, again using pipelines, to control systems and natural gas market operators.[347]

There are over 120 programs operated by private and public organizations to address the six Energy Sector goals mentioned above. These programs fall into one of four categories: information sharing and communications, physical and cyber security,

---

[344] United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*Web.13 Mar. 2011. < http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>
[345] Ibid.
[346] Ibid.
[347] Ibid.

coordination and planning, and public confidence programs.[348] Enumerating all Energy Sector security programs extends beyond the scope and purpose of this paper. It is useful, however, to mention the major programs that exist to counter the threat of Energy Sector terrorism.

Most information sharing and communication programs strive to facilitate security information exchange by creating a "national web-based platform to share homeland security information with sector partners." Examples include public systems, like DHS-IP HSIN, as well as private sector systems like the North American Electric Reliability Corporation's (NERC) ESISAC system. NERC is a not-for-profit, independent organization responsible for ensuring the reliability of the bulk power system in North America.[349] To do that, NERC operates the ESISAC system. ESISAC "receives incident data from private and public entities; assists DOE, FERC, and DHS in analyzing event data to determine threat vulnerabilities and trends; facilitates analysis of incident data and prepares information; disseminates threat alerts, warnings, advisories, notices, and vulnerability assessments;" serves as a liaison between private and public government infrastructure information-sharing centers; and creates awareness about private and public government infrastructure interdependencies.[350] This system exemplifies the public-private Energy Sector relationship, in which there is no distinction made at times between governmental and independent players, as evidenced by this privately owned and operated information sharing network to which the government is a

[348] United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*Web.13 Mar. 2011. < http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>
[349] *North American Electric Reliability Corporation.* Web. 13 Mar. 2011. <http://www.nerc.com/index.php>.
[350] United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*Web.13 Mar. 2011. < http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>

party. Private industry groups for both oil and natural gas are working to establish a similar information sharing system.

Physical and cyber security programs "analyze current security risks and provide information to support effective risk reduction decisions," and to "provide funding for programs that reduce losses from future disasters or help prevent catastrophes."[351] Public confidence programs recognize APPA (American Public Power Association) member utilities that meet stringent guidelines and levels of attainment in the areas of reliability, safety, cybersecurity, mutual aid, disaster management, R&D, and system improvement."[352] Even though this examination of the Energy SSP does not actually include new budget authority to report above the figures reported in the Critical Infrastructure section of this chapter, the threat of energy-sector attacks posed in Chapter One would not be addressed fully without considering these program initiatives.

Cybersecurity

Chapter One identifies several possible attack scenarios, including those involving a breach of U.S. cybersecurity to attack energy systems. Given the documented ability of terrorists and rival nation-state's to infiltrate U.S. information and communication systems, cybersecurity has ascended to a position of high priority for security officials. In May 2009, President Obama issued "The Comprehensive National Cybersecurity Initiative" as a roadmap of current and future cybersecurity initiatives whose purpose is to: ensure a coordinated response to future cyber attacks; strengthen the partnerships

[351] United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*Web.13 Mar. 2011. < http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>
[352] Ibid.

between private and public-sector cybersecurity actors; invest in new technology and research and development to ensure that the U.S. is on the cutting-edge of cybersecurity; and promote cyber awareness and cyber education to build the next generation of technology-savvy cybersecurity operatives.[353]

Although President Obama's cybersecurity outline is helpful to consider as a snapshot of existing and future programs, it is DHS that funds cybersecurity initiatives. There are two sections within the DHS budget dedicated to cybersecurity funding: first, under *Title I: Department Management and Operations,* Office of the Chief Information Officer, "Infrastructure and Security Activities;" and second, under *Title III: Protection, Preparedness, Response and Recovery,* National Protection and Programs Directorate, "National Cyber Security Division."[354] When resources available in these two funding sections are combined, total funding levels for FY2010-FY2007 are: $398,720,000 (FY2010);[355] $345,086,000 (FY2009);[356] $328,796,000 (FY2008);[357] and $288,156,000 (FY2007).[358] When indexed for inflation, funding levels for the series become: $398,720,000 (FY2010); $354,476,933 (FY2009); $338,052,369 (FY2008); and $308,359,762 (FY2007).[359] These figures show a 12.5% cybersecurity funding increase

[353] "The Comprehensive National Cybersecurity Initiative." *National Security Council*, The White House. Web. 14 Mar. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.
[354] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[355] Ibid.
[356] Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/C?c111:./temp/~c111mTqKDx
[357] Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:
[358] Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/ query/z?c109:H.R.5441.enr:
[359] Inflation calculated using CPI data.

from FY2009 to FY2010; a 5% cybersecurity funding increase from FY2008 to FY2009; and a 10% cybersecurity funding increase from FY2007 to FY2008.

President Obama's "Comprehensive National Cybersecurity Initiative" outlines twelve cybersecurity initiatives to be carried out by private and public-sector cybersecurity operatives, but mostly by, or under the supervision of, DHS. The first initiative is to consolidate federal government access points through the Trusted Internet Connections (TIC) initiative, headed by DHS, to reduce the number of external access points, establish baseline security capabilities, and allow DHS to verify agency adherence to baseline security capabilities and standards.[360]

The second initiative is to deploy Intrusion Detection Systems with sensors to detect when unauthorized users are attempting to access federal information sharing networks.[361] DHS currently uses the EINSTEIN 2 capability to monitor Internet activity entering federal systems; EINSTEIN 2 can detect potentially malicious Internet activity with "signature-based sensors."[362] Similarly, the third initiative is to pursue the deployment of EINSTEIN 3 which would prevent intrusions before they occur through real-time monitoring of network traffic entering or leaving Executive Branch networks.[363]

The fourth initiative is to coordinate cybersecurity research and development efforts since "no single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government."[364] This lack of oversight and coordination creates the possibility of wasteful spending and research redundancies. The

---

[360] "The Comprehensive National Cybersecurity Initiative." *National Security Council*, The White House. Web. 14 Mar. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.
[361] Ibid.
[362] Ibid.
[363] Ibid.
[364] Ibid.

fifth initiative is to connect cybersecurity offices and strategic operation centers to enhance information sharing capabilities; ideally this coordination will occur under DHS' National Cybersecurity Center (NCSC) which already exists to secure and facilitate cybersecurity information sharing.[365]

The sixth initiative is to develop a government-wide cyber counterintelligence (CI) plan; this initiative will be addressed by realigning priorities within the intelligence community.[366] The seventh initiative is to increase classified network security, and the eighth initiative is to expand cyber education to create the next generation of cyber security operatives.[367]

The ninth initiative is to develop "leap-ahead" technology, strategies, and programs; these are high-risk/high-payoff research projects.[368] The tenth initiative is to develop enduring deterrence strategies by "improving warning capabilities, articulating roles for private and international partners, and developing appropriate responses for both state and non-state actors."[369] The eleventh initiative is develop a risk-management strategy for global supply chains of commercial information and communications technology that covers the entire lifecycle of products vulnerable for infiltration (such as computer component parts, etc.) that could result in unauthorized access or interruption of communications.[370] Finally, the twelfth initiative is to define the federal role for

[365] "The Comprehensive National Cybersecurity Initiative." *National Security Council*, The White House. Web. 14 Mar. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.
[366] Ibid.
[367] Ibid.
[368] Ibid.
[369] Ibid.
[370] Ibid.

incorporating cybersecurity into the DHS-sponsored critical infrastructure protection plans with private and public-sector stakeholders.[371]

Cybersecurity is clearly a growing sector of homeland security, but not without at least two major negative externalities. First, with added cybersecurity efforts, there is growing concern about protecting civil liberties and the right to privacy. The Government's monitoring of civilian Internet activity is a direct cost for Americans' privacy and civil liberties, and as such, it should be taken into account when considering the cost of cybersecurity. Second, the Government's regulation of the product lifecycle of communications technology, meaning the supply chain, creates a burden for private sector suppliers of communications technology; as well as for communications systems service providers.[372] Security increases as liberty decreases—this is the established relationship between liberty and security in any sector; cybersecurity is no exception.

The Coast Guard, Border/Customs Programs, and Concluding Remarks

The purpose of Chapter Two is to take the threats outlined in Chapter One and to examine: (1) what federal programs exist to address each threat, and (2) how much money the United States spends on those programs (and thus, how much the U.S. spends to address each threat listed in Chapter One). Now that the applicable federal programs have been identified, and costs enumerated, there are still two unaddressed DHS program areas to discuss: The Coast Guard, and Border/Customs programs. Although they may

[371] "The Comprehensive National Cybersecurity Initiative." *National Security Council*, The White House. Web. 14 Mar. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.
[372] Ibid.

address terrorism tangentially, terrorism is not the main focus of the Coast Guard or Border/Customs programs. Thus, because counterterrorism is not the proximate cause for either program area, it would be inappropriate to categorize federal funding for these programs as counterterrorism spending. However, this is a point of some contention, since both the Coast Guard and U.S. border security programs are funded by DHS. To be transparent, therefore, it is worth noting that FY2010 funding for Coast Guard programs was $10,140,291,000,[373] and FY2010 funding for all Border/Customs programs was $12,478,791,000.[374] Should the reader find it appropriate to include either of these funding areas in homeland security funding, she may add those funding totals to aggregate funding levels provided in Chapter Three. This concludes the "cost" section of the U.S. homeland security strategy risk-cost-benefit analysis underway.

[373] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[374] Ibid.

Chapter Three: Benefit

The first two chapters of this thesis outline the terrorism risk to U.S. homeland security and the cost of U.S. anti-terrorism operations. Chapter Three focuses on the "benefits" of homeland security spending by considering the ratio of risk to cost for certain security sectors. In essence, Chapter Three is the "benefit" section of this risk-cost-benefit analysis for U.S. anti-terrorism expenditures.

The primary "benefit" of any security measure is to decrease national susceptibility to terrorism by strengthening anti-terrorism deterrence, prevention and preparedness programs. There are two factors that make it difficult to distinguish program-specific benefits for U.S. anti-terrorism efforts: first, homeland security initiatives do not exist in isolation; all of the programs outlined in Chapter Two operate simultaneously, and thus it is impossible to consider the benefit derived from any one security measure. And second, there is no clear metric, besides instances of terrorism in the United States, to determine which security programs are successful, and which programs are underperforming or are disproportionate to the applicable risk. Notice, both of these factors are true only for citizens and policymakers without access to the internal operations of anti-terrorism programs. Presumably, officials involved in executing security programs can gauge the success of their program based on the appropriate standard with respect to their program-specific anti-terrorism mission (e.g. number of terror plots foiled, terrorist detained, etc.).

The success or failure of terrorism is dependent upon an array of situational factors, some of which are controlled by terrorists, others of which are controlled by the target country, and others still which are entirely random (such as the weather for a

bioterrorist attack). Despite the multiplicity of factors dictating the success or failure of terrorism, U.S. homeland security officials tout the success of increased security efforts based on the fact that there has not been another large-scale terrorist attack since 9/11. While it is psychologically soothing to attribute the absence of large-scale terrorism to U.S. homeland security measures, there is no way to confirm or deny the inverse relationship between security efforts and large-scale terrorism. Without a metric to gauge the success of individual security measures, policymakers never demonstrate the value of threat-specific security programs to the uninformed general public. This means that the electorate can neither verify nor disprove the necessity of security efforts at current funding levels. For the ordinary citizen or policymaker, then, it is impossible to judge the marginal gain, or the benefit, to U.S. homeland security of specific programs.

Thus, the concept of "benefit," with respect to U.S. homeland security programs, must be redefined. Instead of thinking about benefit as an increase in security, this paper will consider benefit as addressing the known risk of terrorism, and to the appropriate degree (meaning the degree to which threat-specific security programs are in proportion to the security risks they address). Chapter Three, therefore, will use the threat analysis of Chapter One (risk), in light of the data outlined in Chapter Two (cost), to determine whether several existing U.S. homeland security sectors have a positive, negative, or neutral benefit for national security.

To address the threats outlined in Chapter One, Chapter Two identifies eight security sectors: Intelligence, First-Responders, Secret Service, Transportation Security, Critical Infrastructure Protection, Chemical and Biological Weapons Programs, Nuclear and Radiological Weapons Programs, and Cybersecurity Programs. Funding levels for

these security sectors for FY2010 were: $53,100,000,000 (Intelligence); $12,178,670,000 (First-Responders); $522,113,000 (First-Responders Emergency Communications Systems); $2,957,338,000 (Secret Service); $7,656,066,000 (Transportation Systems); $2,058,993,000 (Critical Infrastructure); $366,681,000 (Chemical and Biological Weapons Programs); $30,040,540,000 (General Nuclear and Radiological Weapons Programs) plus $150,188,000 (DHS Nuclear and Radiological Weapons Programs); and $398,720,000 (Cybersecurity Programs).[375] When funding levels for each of these programs are consolidated, the total U.S. homeland security budget for FY2010 was $109,429,309,000. It is important to note that this figure includes programs with multiple missions, but for which the primary mission is counterterrorism. Thus, this figure may include some funding that is not actually used for counterterrorism, but it is impossible to distinguish those funds from aggregate expenditures.

Using $109,429,309,000 as the total budget authority for all domestic anti-terrorism programs, it is then possible to determine what percentage of total funding was allotted to each security sector, and thus to establish the priority afforded to each sector. For all security appropriations for FY2010, Intelligence Programs received 48%, Nuclear and Radiological Programs received 28% (when general program funding and DHS program funding is combined), First-Responder Programs received 11.1%, Transportation Security Programs received 7%, The Secret Service received 2.7%, Critical Infrastructure Programs received 2%, Emergency Communications Systems

[375] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

Programs received 0.5%, Cybersecurity Programs received 0.36%, and Chemical and Biological Weapons Programs received 0.34%.

Rank	Security Sector	Percentage of Total FY2010 Security Funds
1	Intelligence	48%
2	Nuclear/Radiological	28%
3	First-Responders	11.1%
4	Transportation Security	7%
5	Secret Service	2.7%
6	Critical Infrastructure	2%
7	Emergency Communications Systems	0.5%
8	Cybersecurity Programs	0.36%
9	Chemical/Biological	0.34%

There are four points to make about the homeland security spending distribution for FY2010. First, intelligence spending represents nearly half (48%) of all security funding. While $53.1 billion appears to be an inappropriately large sum to spend on non-military intelligence, it may actually be an efficient use of federal funds. Second, nuclear and radiological weapons programs receive the second largest portion of federal funding (28%); this does not correlate with the threat posed by atomic terrorism. Although some nuclear and radiological weapons programs serve non-counterterrorism missions, total funding for these programs is so large that, even if a significant portion went towards traditional purposes, there would still be a disproportionately large sum dedicated to nuclear anti-terrorism programs. Furthermore, even though certain nuclear weapons

programs serve non-counterterrorism missions those programs may nevertheless contribute to anti-terrorism efforts. With any nonproliferation program, there is no clear distinction between traditional safety missions and anti-terrorism missions since general nuclear security also contributes to atomic terrorism prevention. Thus, this paper acknowledges that nuclear programs entail non-counterterrorism initiatives, but nevertheless uses total nuclear funding since it is unclear exactly which initiatives should be classified as anti-terrorism measures versus traditional nonproliferation measures.

Third, bioterrorism prevention programs, which receive only 0.34% of all federal security dollars, are inadequate. Though bioterrorism is not the most pressing security risk, the lack of U.S. preparedness for this mode of terrorism creates unnecessary risk and thus bioterrorism prevention should be more of a national security priority. And finally, cyberterrorism is a rapidly emerging and significant threat, and yet it receives only 0.36% of federal homeland security funds. Cyberterrorism must become more of a security priority since the risk of cyber attack increases with the passage of time. With both bioterrorism prevention and cybersecurity, it is unclear whether additional homeland security funds would result in increased national security. Experts point to obvious holes in both bioterrorism prevention and cybersecurity systems, but increasing biosecurity and cybersecurity budgets may be unnecessary and, without access to operational information, it would be groundless to prescribe funding increases here. Thus, this paper merely identifies the security vulnerabilities in these areas and recommends addressing the risk created by flawed security systems. The remainder of this chapter will focus on these four points and will conclude with a brief analysis of U.S. anti-terrorism funding levels in FY2010 relative to other U.S. budget priorities and national wealth.

As noted above, non-military intelligence spending for FY2010 was $53.1 billion, which represents 48% of all U.S. homeland security funding. Intelligence is the largest recipient of federal security funds for two reasons: first, intelligence programs are responsible for providing information services to a large number of agencies with missions beyond counterterrorism; and second, because policymakers understand that "good intelligence is the best weapon against international terrorism."[376] The single most effective way to prevent terrorism is to ascertain accurate information about the identity, plans, goals, and vulnerabilities of terrorists and terrorist organizations.[377] This is because there are an infinite number of possible targets and means for terrorism, and thus protecting infrastructure is far less effective than preempting attacks by gathering timely and accurate information.

Intelligence programs are obviously necessary, but it is impossible for an individual without a security clearance to determine whether U.S. intelligence expenditures are efficient. This is because intelligence spending, beyond aggregate spending totals, is classified. There are numerous reports expressing the need for more human intelligence sources to counter terrorism. One Congressional Research Service report notes that counterterrorism is "especially dependent" on human intelligence sources and "depends on contacts with sources far removed from embassy gatherings and requires expertise in languages that are possessed by few in this country."[378] Without

---

[376] "*Good Intelligence is the Best Weapon Against International Terrorism"* Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism, Pursuant to Public Law 277, 105th Congress

[377] Ibid.

[378] Best, Richard A., Jr. *Intelligence Issues for Congress*. Congressional Research Service, 3 Mar. 2011. Web. 30 Mar. 2011. <http://www.fas.org/sgp/crs/intel/RL33539.pdf>.

knowing how much money is already spent on gathering human intelligence, or on linguists, it is impossible to gauge the necessity or efficiency of current spending levels.

There are two additional facets of U.S. intelligence programs that make it difficult to determine whether intelligence funds are well spent. First, intelligence operations are classified, and thus, there is no way to determine whether intelligence programs reflect genuine risk. For example, the general public cannot look up how many terrorist plots are discovered annually; there is only anecdotal evidence in the media from which to approximate the number of CIA and FBI interventions. Thus, for the general public, there is no way to distinguish good intelligence investments from bad intelligence investments. This is problematic because it is impossible to check federal policymakers without the relevant information. The democratic system breaks down when the electorate does not have access to the necessary information to form an opinion of security spending, and thus congressional representatives act illegitimately.

The second factor that complicates an analysis of the value of intelligence spending is the civil liberty cost associated with intelligence gathering. To allow information to flow more freely between the FBI and the CIA, Congress passed the PATRIOT Act in 2001. The purpose of the PATRIOT Act was to implement an "all-service intelligence effort against terrorist groups inside and outside the U.S.;" but the *de facto* result was an invasion of privacy for U.S. citizens. There is, then, a cost for U.S. intelligence programs paid by the sacrifice of individual civil liberties. As noted in Chapter Two, negative externalities, like reduced civil liberties, are not true "costs" because they cannot be quantified. Nonetheless, negative externalities are real in that their presence has a palpable and detrimental impact much like quantifiable cost. Yet,

without knowing the effectiveness of U.S. intelligence programs, it is impossible for Americans to determine whether the price of intelligence (meaning reduced civil liberties) is justified by an equal increase in security.

Thus, all that may be said with certainty about the amount of money the United States spends on non-military intelligence programs is that, in general, experts agree that intelligence is the best way to counter terrorism, and that there have been complaints about inadequate human intelligence for anti-terrorism programs. There is very little that can be said, however, about the value of intelligence programs based on their success in discovering terrorists; and there is even less that can be said about the value of intelligence programs that directly violate civil liberties, since nothing is known about the productiveness of those programs. This lack of transparency would be more acceptable if there was a smaller amount of money involved, but because intelligence programs are the highest funded sector of U.S. homeland security, there must be an effort to disclose more information to the general public about how intelligence funding is spent to justify the financial and social costs for this security sector.

Nuclear nonproliferation and defense programs are the second highest funded security sector, receiving 28% of all security appropriations. Judging the efficiency of atomic terrorism prevention programs is complicated by the fact that the risk of a nuclear attack is miniscule, and yet the catastrophic consequences of such an attack make even a small risk of nuclear proliferation unacceptable. The devastation of a nuclear attack would be profound, both economically and politically, but current spending levels for nuclear prevention programs are disproportionately high relative to all but the most extreme scenarios (which are essentially impossible). This is because the possible paths

for terrorist groups to acquire or create nuclear weapons are riddled with serious obstacles, and when considered together, the accumulation of these obstacles renders them likely insurmountable.

The best way to conceptualize how truly small the probability is of atomic terrorism is to review the steps necessary to acquire or create a nuclear weapon. There are only three routes to atomic terrorism. A terrorist organization could: (1) acquire a completed nuclear weapon from a nuclear state; (2) steal or illicitly purchase a nuclear weapon; or (3) build its own nuclear weapon.[379] The first path, acquiring a nuclear weapon from a sympathetic nuclear state, is often discussed with respect to Pakistan and North Korea. This scenario is unlikely, however, because with the advent of nuclear forensics (which allows investigators to connect the nuclear material used in an atomic weapon to its source) the origin of the nuclear material used by terrorists would be discovered, and the wrath of the international community would be swift and exacting. In short, any nuclear state willing to provide terrorists with an atomic weapon might as well detonate that weapon directly since the result is the same.

Some issue experts are concerned about the possibility of private nuclear weapons contracting by technocrats willing to sell their expertise to terrorist organizations. For example, Pakistani scientist A.Q. Khan is known to have sold his nuclear weapons expertise to both North Korea and Iran.[380] This is a distorted conception of that threat, however, since even the opportunistic Khan never aided terrorists; he only took nation states as clients, and his operation was easily discovered and shutdown by U.S.

---

[379] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[380] Ibid.

intelligence services.[381] This distinction is important since, unlike terrorists, nation states desire nuclear weapons to create prestige or leverage within the international community; most nuclear states do not actually intend to detonate their nuclear devices. There may be an exception to this general rule, such as a truly belligerent state like Libya today, but the United States has successfully countered the threat of state-sponsored atomic terrorism in the past (e.g. the Cold War). Atomic terrorism by non-state actors, however, is an entirely different threat since the United States' ability to counter atomic terrorism by non-state actors is markedly different, and arguably more complicated, than the United States' ability to prevent state-sponsored atomic terrorism.

The second path to atomic terrorism is for a terrorist group to steal or illicitly buy a nuclear weapon. Experts devised two possible scenarios for stealing a nuclear weapon: first, terrorists could steal a "loose nuke" allegedly in circulation in former Soviet bloc nations; and second, a terrorist group could infiltrate the nuclear facilities of a state and steal a nuclear weapon or the nuclear material for a weapon.[382] The first scenario is highly contentious since Russian nuclear officials and Russian nuclear program experts vehemently deny that Al Qaeda or any terrorist organization could have acquired Russian atomic weapons.[383] The same experts also point out that, even if a terrorist organization did have a loose Russian nuke, all of the Soviet nuclear weapons were constructed before 1991, and since nuclear weapons are very difficult to maintain and have a lifespan of one to three years, no Soviet loose nukes would be viable today.[384] Also, Russia has a vested interest in securing any loose nukes, as Russia is the likely target of atomic terrorism if

[381] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[382] Ibid.
[383] Ibid.
[384]Ibid.

loose nukes were acquired by Chechen terrorists. For these reasons the fabled Soviet loose nuke threat seems to be more myth than fact.

Some experts also worry that a nuclear state will fail, such as North Korea or Pakistan, and then that nuclear material could fall into the hands of terrorists. This scenario is also unlikely because, were a nuclear state to fail, the international community would move quickly to secure nuclear material. Additionally, for a terrorist organization to take advantage of a failing state, they would have to strike at precisely the right moment, work in perfect harmony to transport the weapon without discovery, and find a covert storage facility to avoid international detection.

It is also possible that a terrorist organization could steal a nuclear weapon or nuclear material from a stable nuclear state. This scenario is unrealistic since nuclear facilities are well protected, and because even if infiltrated, nuclear states would immediately notice the missing material and would work to recover the nuclear material. There is every reason to believe that the violated nuclear state would launch an immediate and feverish investigation for the same reasons that a nuclear state does not give terrorists nuclear materials: because nuclear material is easily traceable, and the nuclear state would not want to be held responsible for a nuclear incident originating from their nuclear material.[385]

The third, and most likely, path to atomic terrorism is for a terrorist organization to construct a nuclear weapon. This scenario is the most likely scenario because of the issues associated with receiving, stealing, or illicitly buying a nuclear weapon outlined above. Plutonium and uranium are the two options for obtaining the fissile material

[385] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.

needed to construct a nuclear weapon. Because of the dangers of working with and transporting plutonium, terrorists would almost certainly choose to work with highly enriched uranium (HEU).[386]

To construct a weapon, terrorists would have to collect as much HEU as possible, and then use that material to build a nuclear device. Because of the complexity of transporting the nuclear device from the production site to the target site, the nuclear device would probably not be sophisticated enough to be able to be dropped or launched, but rather would be a simple design that could be detonated by suicide terrorists at the target site.[387] Even this, the simplest scenario, requires terrorist organizations to overcome significant obstacles at every stage of production.

To illuminate just how difficult constructing a nuclear weapon is, consider the process terrorists would have to undergo to accomplish a rudimentary atomic weapon. First, fissile material can be either produced or procured. Terrorists would not be able to produce HEU since to do so would require an industrial scale effort that would be impossible to conceal, if it were even possible for a terrorist group to orchestrate.[388] As with nuclear weapons, states are unlikely to give terrorists fissile material since it can be traced back to the state; thus, terrorists would have to steal or illicitly purchase HEU.[389]

It is very unlikely that terrorists would be able to steal HEU because fissile material is kept under tight surveillance and thus authorities monitoring fissile material would realize if HEU were missing. In fact, "known thefts of highly enriched uranium have totaled fewer than 16 pounds or so. That amount is far less than that required for an

---

[386] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[387] Ibid.
[388] Ibid.
[389] Ibid.

atomic explosion for a crude bomb, over 100 pounds are necessary to produce a yield of one kiloton."[390] Furthermore, of the known thefts, none were committed by AQ, none of the thieves had buyers lined up before the robbery operation, and almost all of the thieves were caught when they tried to sell the stolen HEU.[391]

For the purpose of demonstrating the inherent obstacles facing would-be atomic terrorists, assume terrorists succeeded in acquiring enough HEU for an atomic weapon, either through theft or illicit transactions. They would then have to transport their contraband back to their base of operations to construct a weapon. Given the amount of HEU required to make a nuclear device, the HEU would probably be coming from multiple locations, which creates tremendous risk that, at some point in the transportation process, some of the HEU will be detected by customs or border security.[392]

Again for the sake of the argument, assume also that terrorists find a means to evade border security, and transport all of the necessary HEU back to their base of operations, there is still the issue of actually constructing the nuclear devise. To make an atomic weapon, terrorists would have to set up a large, technically advanced facility, and populate it with skilled technicians, scientists and mechanics.[393] If the facility was not detected by citizens, local security authorities, or international security agencies, then the terrorists would also need detailed instructions to build a nuclear bomb (a very dangerous task), as well as, a constant supply of electricity and reliable access to tools and supplies.[394] If these conditions could be achieved, terrorists would also need months, if

---

[390] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[391] Ibid.
[392] Ibid.
[393] Ibid.
[394] Ibid.

not a year or more, to construct the weapon, during which time the operation would have to avoid detection.

If a terrorist organization were to produce a nuclear weapon, they would still need to transport that weapon to the target site. This would be challenging since any nuclear devise would have to be concealed in lead shielding to hide radioactive emissions, which would mean that the weapon would weigh a ton or more.[395] Terrorists would have two options for transporting the atomic bomb. First, they could use the commercial transportation system, which would essentially supply authorities with a return address for the weapon, and hope transportation authorities do not detect the nuclear weapon.[396] Or, alternatively, they could hire an aircraft or use established smuggling routes which would require the absolute reliability and loyalty of a cadre of accomplices.[397] If the nuclear devise were to be successfully transported, it would then have to be received by technically skilled terrorists capable of maintaining the devise and transporting it, using public roads, to the target site without detection.[398]

In addition to these obstacles, there is also the financial burden of producing a nuclear weapon to consider. Creating or buying a weapon involves significant investments in materials, human capital, and in transportation and concealment costs. Terrorists with the amount of money necessary must also be willing to expend that amount of money on an attack plan with a very low probability of success. To quantify just how low the chance is of executing a successful atomic attack, CATO Institute nuclear terrorism expert, John Mueller, identifies 20 obstacles standing between willing

---

[395] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[396] Ibid.
[397] Ibid.
[398] Ibid.

terrorists and an atomic weapon, all of which are mentioned above. Next, Mueller gives terrorists a very generous 50% chance of overcoming each of the 20 obstacles. Given those odds, there is a 1-in-1,048,576 chance of success for terrorists.[399] Mueller recognizes that a 50% chance of overcoming each obstacle is unrealistic, so to better reflect reality, Mueller runs a second model in which he gives terrorists a one-in-three chance of overcoming each of the 20 obstacles. Given those odds, there is a 1-in-3,486,784,401 chance that terrorists will successfully execute a nuclear attack.[400]

This analysis is not meant as an argument against all nuclear weapons prevention programs; rather, it is meant to contextualize nuclear spending. Any nuclear event would have catastrophic consequences—there is literally no greater risk to the United States in terms of potential financial and human losses. However, the risk of such an attack is miniscule. Thus, policymakers must address the threat, but not give into alarmist scenarios that inflate the risk of atomic terrorism to justify spending 28% of all security funds on nuclear prevention. Again, some nuclear prevention programs serve broader security purposes than strictly counterterrorism, but that does not justify current spending levels. Nuclear terrorism is a threat worth preventing, but the response to this threat cannot be hugely disproportionate to risk, especially when U.S. security funds are limited and greater threats to U.S. homeland security exist that are not given adequate resources.

Bioterrorism is one such example of a financially underrepresented risk to U.S. homeland security. In FY2010, bioterrorism was allocated just 0.34% of all federal

[399] Mueller, John. "The Atomic Terrorist?" *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 139-160. Print.
[400] Ibid.

security funds, or $366,681,000.[401] In 2005, Interpol, the leading international security agency, hosted a bioterrorism conference in France to galvanize attending nations to develop bioterrorism prevention programs. At that conference, Ronald K. Noble, the Secretary General of Interpol, said: "Heads of government, the United Nations, the World Health Organization, heads of police intelligence services, counter-terrorism experts and we at Interpol all agree that the threat of bioterrorism is real and present."[402] In fact, Noble went so far as to describe the threat of a bioterrorist attack as the greatest "potential danger to all countries, regions and people."[403] AQ has indicated that the group intends to use biological agents in a massive terrorism event, and even posted instructions to create a biological weapon online.

The threat of bioterrorism is not the most pressing concern for the United States because biological agents are difficult to weaponize, and thus other, cruder weapons like IEDs are more likely to be used in terrorist attacks. That said, bioterrorism is a genuine threat, as indicated by Interpol, and the United States is unprepared to counter it. In recent years, there has been an effort to improve the U.S. bioterrorism prevention strategy by implementing widespread biosurveillance. There are two purposes of biosurveillance: first, to detect a potentially dangerous biological event as soon as possible; and second, to improve the quality of information available about a biological incident to increase

[401] DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.
[402] Noble, Ronald K. "Opening Remarks." *Preventing Bio-Terrorism: The First Interpol Global Conference*. Web. 30 Mar. 2011. <http://www.interpol.int/Public/ICPO/speeches/NobleBioTerrorism20050301.asp?HM=1>.
[403] Ibid.

situational awareness and to guide the national response to such a biological event.[404] Even though biosurveillance is the largest aspect of the U.S. anti-bioterrorism strategy, implementation of this tool has been retarded by a lack of centralized leadership and funding. The Government Accountability Office (GAO) describes the current status of the U.S. anti-bioterrorism strategy as incomplete: "While national defense strategies have been developed to address biological threats such as pandemic influenza, there is neither a comprehensive national strategy nor a focal point with the authority and resources to guide the effort to develop a national biosurveillance capability."[405]

To sufficiently address the threat of bioterrorism, the U.S. must develop a strong, integrated biosurveillance capability. Without access to operational information, all that is known about current bioterrorism prevention efforts is that the United States has insufficient biosurveillance capabilities. What is unclear, however, is whether additional resources would help expedite the biosurveillance implementation process. Components of the biosurveillance implementation process point to the lack of centralized leadership to disseminate responsibilities and to oversee the implementation of a biosurveillance system as the reason for inadequate biosureveillance, but additional funding will not fix this organizational problem. There may also be a need for additional resources, but enlarging the bioterrorism budget should happen only after organizational problems are addressed. Going forward, Congress should condition bioterrorism prevention funds upon the reorganization of DHS efforts to implement biosurveillance capabilities. Congress should also identify leadership and agency responsibilities and institute deadlines for

[404] Jenkins, William O., Jr. *BIOSURVEILLANCE: Preliminary Observations on Department of Homeland Security's Biosurveillance Initiative.* The Government Accountability Office, 16 July 2008. 30 Mar. 2011. <http://www.gao.gov/new.items/d08960t.pdf>.
[405] Ibid.

biosurveillance implementation. Bioterrorism is a complex mode of terrorism, and it is unlikely that the United States will be the victim of a large-scale biological terrorist attack. But as the anthrax mailings of 2001 demonstrate, bioterrorism is possible, and the United States' current inability to counter this risk creates unnecessary and unacceptable vulnerability.

Cyberterrorism continues to emerge as a threat to U.S. homeland security, and like bioterrorism, it is a vulnerable security sector. The most significant cybersecurity risk is the infiltration of federal information sharing systems; particularly since government systems are increasingly interconnected.[406] This threat is not only realizable, but it is also gaining momentum: from FY2006 to FY2009, cybersecurity incidents increased by over 400-percent.[407] The GAO has made several recommendations to strengthen national cybersecurity including fully-implementing the Federal Desktop Core Configuration Initiative; requiring delinquent agencies to execute their agreements with DHS to use the Einstein computer network detection system; and requiring delinquent agencies to meet the requirements for the Trusted Internet Connections Initiative.[408]

The most common recommendation, however, is to fully-implement the twenty-four policy improvements outlined in 2009 by the commission appointed by President Obama to investigate Bush-era cybersecurity programs. In 2008, the Bush Administration created the Comprehensive National Cybersecurity Initiative (CNCI) to improve cybersecurity within government information sharing systems. Then, in 2009, President Obama ordered a review of the national cybersecurity strategy, with emphasis on

---

[406] Wilshusen, Gregory C. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*. The Government Accountability Office, 16 Mar. 2011. Web. 30 Mar. 2011. <http://www.gao.gov/new.items/d11463t.pdf>.
[407] Ibid.
[408] Ibid.

government systems. That review yielded twenty-four policy recommendations to improve national cybersecurity. Of those twenty-four recommendations, only two have been fully implemented.[409]

The GAO investigated implementation efforts for these twenty-four initiatives to determine why the implementation process was moving so slowly. The investigation revealed that the agencies responsible for implementation –primarily DHS, DOD, and OMB—were struggling to progress because they have not been assigned roles or responsibilities for implementing the broad, long-term recommendations.[410] Investigators also found that sixteen of the twenty-two partially implemented recommendations do not even have identifiable milestones or defined plans for implantation.[411]

GAO investigators concluded that, until there are assigned roles and responsibilities for all agencies involved, as well as milestones and clear implementation plans, "there is increased risk the recommendations will not be successfully completed, which would place the country's cyber infrastructure at risk."[412] Cybersecurity may well be the Achilles' heel of the U.S. homeland security strategy—especially since experts agree that, as terrorist organizations gain computing sophistication, the threat of cyber attack will only increase with time. As noted in Chapter Two, many assets listed as critical infrastructure require information sharing system, and are interconnected through common computer networks. This means that vulnerabilities to cyber infrastructure would have particularly dire consequences for the energy sector, intelligence programs,

---

[409] Wilshusen, Gregory C. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*. The Government Accountability Office, 16 Mar. 2011. Web. 30 Mar. 2011. <http://www.gao.gov/new.items/d11463t.pdf>.
[410] Ibid.
[411] Ibid.
[412] Ibid.

emergency responders, and a host of other agencies. For this reason, it is imperative that U.S. policymakers make cybersecurity more of a priority and oversee the implementation of all policy recommendations. Unlike bioterrorism, where vulnerability may simply be the product of mismanagement, cybersecurity is weak and will require robust tools to secure government networks. This may require more than the current spending level of $398,720,000, or 0.36% of total federal security dollars; and it certainly requires full participation from implicated government agencies and additional leadership with the authority to force agency compliance to cybersecurity protocols.

Comparing U.S. security spending levels in a vacuum is useful insofar as it demonstrates national security priorities; but it conveys very little about the appropriateness of aggregate U.S. anti-terrorism spending. This is because the appropriateness of anti-terrorism expenditures is relative not only to risk, but also to total federal expenditures and to national wealth. The purpose of considering total federal expenditures is twofold: first, it provides a scale for security funding. There is no way to judge the reasonableness of security funding without knowing the total amount of money the United States spends annually. For example, $109,429,309,000 (total U.S. security spending) could be an enormous amount of money or it could be a miniscule amount depending on how much money is spent on all other programs. Second, considering total federal expenditures allows the observer to determine federal funding priorities and thus to contextualize security funding relative to other sectors. It is important to understand security funding relative to other sectors because security funding levels are appropriate if, and only if, they are proportional to the funding levels of other federally funded sectors of the economy. For example, $109,429,309,000 is not an appropriate amount of

money to spend on anti-terrorism programs if total U.S. healthcare expenditures are less than that amount. Finally, it is important to consider security funding relative to national wealth (measured in gross domestic product for this paper) because the appropriateness of U.S. anti-terrorism expenditures depends on total national wealth. If, for example, annual security funding amounts to more than the annual gross domestic product (GDP), then security programs receive an inappropriately large amount of money. The following analysis, then, considers FY2010 security funding relative to (1) total federal expenditures for FY2010, and (2) GDP for 2010.

Total federal expenditure for FY2010 was $3.456 trillion.[413] Most of the federal budget is consumed by four sectors: Defense, Healthcare, Pensions and Welfare. In FY2010, Defense programs received $847.2 billion or 25% of all federal outlays.[414] Healthcare received $820.7 billion in FY2010, or 24% of all federal outlays.[415] In FY2010, Pensions received $749.6 billion or 22% of total federal expenditures for that year.[416] And finally, Welfare received $502.3 billion in federal funding or 15% of all FY2010 federal expenditures.[417] The rest of the federal budget for FY2010 was consumed by Interest on public debt ($196.2 billion), Protection ($53.4 billion), Transportation ($92 billion), General Government ($24.7 billion), and Other Spending ($29.7 billion).[418] In FY2010, the United States spent $109,429,309,000 on anti-terrorism measures; this represents 3.17% of all budget outlays for that year. The conclusion to draw here is that, on the continuum of federally funded sectors, homeland security

[413] Chantrill, Christopher. "FY2010 Government Spending Details ." *U.S. Government Spending*. Web. 10 Apr. 2011. <http://www.usgovernmentspending.com/piechart_2010_US_fed>.
[414] Ibid.
[415] Ibid.
[416] Ibid.
[417] Ibid.
[418] Ibid.

programs fall in between the major and the minor components of the budget: anti-terrorism funding is less than Defense, Healthcare, Pensions and Welfare, but greater than Transportation, General Government, and Other Spending. Without regard for the quantity allocated, this is an appropriate place for anti-terrorism measures to fall. Homeland security should be a national priority, but it is not the supreme priority.

Similarly, GDP for 2010 was $14.66 trillion.[419] Thus, in 2010, federal expenditures as a percentage of GDP were as follows: Defense, 5.78% of GDP; Healthcare, 5.6% of GDP; Pensions, 5.1% of GDP; and Welfare, 3.4% of GDP. For 2010, anti-terrorism programs represented 0.746% of GDP; this is even less than the interest owed on public debt in 2010, which represented 1.34% of GDP. France, and other European nations designate 1% of GDP to be the appropriate amount to spend on anti-terrorism efforts.[420] Current U.S. homeland security expenditures are slightly less than 1% of GDP, but are close enough to that target to be considered an appropriate percentage of total national wealth, as defined by the European model.

There are two additional points to make here: first, U.S. anti-terrorism measures are not a significant federal investment relative to the four largest consumers of federal funds (Defense, Healthcare, Pensions, and Welfare). This is appropriate, however, because anti-terrorism programs do not have the same manifest benefit and necessity as these other four sectors. Homeland security measures counter unknown, emerging, and unlikely threats; thus, the benefit and necessity of security programs are debatable. Defense, Healthcare, Pension and Welfare programs, however, serve at least large

---

[419] Chantrill, Christopher. "FY2010 Government Spending Details ." *U.S. Government Spending*. Web. 10 Apr. 2011. <http://www.usgovernmentspending.com/piechart_2010_US_fed>.

[420] Archick, Kristin, et al. *European Approaches to Homeland Security and Counterterrorism*. Congressional Research Service, 24 July 2006. Web. 30 Mar. 2011. <http://www.hlswatch.com/sitedocs/RL33573.pdf>.

segments of the population – if not the entire population (as with Defense programs). Thus, it is reasonable to make anti-terrorism programs less of a national priority than Defense, Healthcare, Pensions, and Welfare since, unlike these other sectors, the marginal benefit and necessity of anti-terrorism programs is ambiguous.

The second point to make is that with federal expenditure, comes federal deficit and public debt. The federal deficit for FY2010 was $1.3 trillion and the gross public debt in FY2010 was $13.5 trillion.[421] Deficit and debt considerations compound the problem of how to prioritize anti-terrorism spending. Now, instead of a merit-based question (i.e., *should* the United States fund anti-terrorism efforts at current levels?), the growing federal deficit and debt change the consideration to an ethics-based question (i.e., can the United States *afford* to fund anti-terrorism efforts at current levels?). Going forward, policymakers will likely have to cut spending to make U.S. debt sustainable. The important thing to note from this comparison of anti-terrorism measures relative to total expenditure and GDP is that it is appropriate for anti-terrorism measures fall below the largest sectors of the economy, but above lesser priority sectors. Thus, in the event of a major budget recalibration, the current budget prioritization should remain; there should be across-the-board cuts to all sectors, including homeland security.

Concluding Remarks

The purpose of this thesis is to determine the accuracy of the risk assessment model used by U.S. policymakers to allocate homeland security funds. Unfortunately, any risk-cost-benefit analysis for U.S. homeland security is clouded by the fact that,

[421] Chantrill, Christopher. "FY2010 Government Spending Details ." *U.S. Government Spending*. Web. 10 Apr. 2011. <http://www.usgovernmentspending.com/piechart_2010_US_fed>.

without a security clearance, there is no ability to discern how certain security sectors spend federal funds. This analysis is also encumbered by the fact that, even when funding levels are not classified, spending reports are not centralized in one location. To get a snap shot of homeland security spending, the observer must piece together spending information from a host of various agency websites, from appropriation bills, from governmental and non-governmental think-tank studies, and from analyses by government watch-dog organizations. This lack of transparency is understandable to a degree, since terrorists also look to define U.S. homeland security expenditures, but there must be more of an effort to inform the American electorate about security programs when divulging operational and funding information does not endanger national security.

Despite roadblocks created by the sensitive nature of security spending, it is possible to point to four issues that deter accurate risk assessment for U.S. policymakers allocating security funds. First, preventing atomic terrorism involves countering a threat with a very low probability but very large consequences, and "the tendency has been to overestimate both probability and consequences."[422] Second, terrorists put considerable time and effort into planning attacks for which the United States is unprepared; thus, any effort to predict risk based on previously observed threats is inherently outdated.[423] Some threats persist, such as suicide bombers, but target selection, modes of terrorism, and even terrorist groups continually evolve to encompass knew, unknown scenarios making risk assessment essentially a moving target. Third, homeland security risk assessments seem to discount the economic effects of security programs. Some pervasive security

[422] Lewis, James A. "Assessing Counterterrorism, Homeland Security, and Risk." *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 83-97. Print.
[423] Ibid.

measures inhibit commerce, require private markets to meet governmental standards that are not economically efficient, and increase the cost of doing business in the United States; while other programs are stimulatory, adding to domestic prosperity by creating jobs for a technically skilled labor force.[424] Fourth, the politicization of homeland security appropriations allows fear mongering and pork barreling to eclipse actual risk, leading to distorted national security priorities. Because it is impossible to predict future terrorist attacks, it is easy for alarmists to inflate the perceived risk of low-probability threats. This, in turn, allows Congress to spend heavily to prevent unlikely threats while accumulating goodwill from those positively affected by increased security spending. Normally, wasteful spending is checked by reports of inefficient expenditures, but "because the threats [the U.S. is] defending against are so improbable, we have little ability to measure the benefit of a program other than by how much is spent on it. We can spend large sums of money without substantially reducing the risk of an attack."[425]

The United States historically equates increased expenditure with increased security, which is perhaps why the U.S. spends "more than most other nations combined to prepare for attacks."[426] In fact, some critics of current security spending levels claim that terrorism preparation has become a means of federal subsidy, removed entirely from genuine risk assessment models.[427] These critics point to the federal grant funding received by "the Amish Country Popcorn Company" in Indiana, which has a population of 4,200; and to the fact that Florida's "City of Mermaids" was designated as critical

[424] Lewis, James A. "Assessing Counterterrorism, Homeland Security, and Risk." *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 83-97. Print.
[425] Ibid.
[426] Ibid.
[427] Ibid.

infrastructure; and to a state agency in Kentucky that was awarded grant funding to "prevent terrorists from using bingo games to fund their operations."[428] These examples are obviously egregious outliers, but they nonetheless demonstrate the point that, instead of reflecting the intelligence community's assessment of realistic national security concerns, grant funding *can* become a means of earmark spending.

Without access to intelligence data, there is no way of knowing how many plots the U.S. disrupts annually, nor if terrorist plots are actively deterred by homeland security measures. It is possible, however, to point to the failed terrorist attacks occurring from 2009-2010 as evidence that America is clearly not as safe as security budgets indicate. This risk-cost-benefit analysis determined that intelligence spending is markedly greater than any other security sector, and that very little publicly available information exists about how intelligence funds are spent; that nuclear prevention programs are over-funded relative to the actual risk of an atomic terrorist event; that biological terrorism, though perhaps not as likely as other modes of terrorism, is underfunded; and that cybersecurity is underfunded given the emerging, unaddressed nature of that threat. The remaining question, then, is what improvements can be made to adjust the federal homeland security risk-cost-benefit analysis.

There are several policy considerations that, if implemented, would improve the accuracy of homeland security risk assessment and the efficiency of security appropriations. First, with respect to terrorist target selection, policy makers must be aware that there are an infinite number of potential terrorist targets. Admittedly, some targets are more appealing based on their national importance, but those targets have been

[428] Lewis, James A. "Assessing Counterterrorism, Homeland Security, and Risk." *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 83-97. Print.

hardened by increased security measures, and thus are less likely to be the target of a successful terrorist attack. Once the most obvious targets, like the Pentagon, are discounted, other targets are essentially random. Terrorists select their targets based on convenience or because they have knowledge of the specific layout or intricacies of their target. The large amount of federal funding dedicated to "protective measures" indicates that policymakers have not internalized the fact that possible terrorist targets are infinite. Protective measures are passive defense efforts, such as "posting security guards, hardening targets against explosions, screening people entering an area, setting up barriers, and installing security cameras."[429] These efforts might be useful in preventing pedestrian crime, but they represent only marginal gains in homeland security.

Target selection has historically been even more random for homegrown terrorism. Former Director of the FBI, Robert Mueller, warns that homegrown terrorists are the most likely perpetrators of future acts of terrorism; given the access and proximity advantages they hold living in the United States.[430] Mueller also notes that domestic terrorists choose targets "for their convenience."[431] Instances of homegrown terrorism, whether successful or not, involve targets familiar to the terrorists. This creates an element of randomness that disallows the prediction of future targets, and thus forecloses the opportunity to harden likely targets through increased security measures. International terrorists may focus on iconic targets, perhaps because they are unfamiliar with non-iconic U.S. assets, but as indicated by trends established over the last few years, incidents of domestic terrorism are more likely to be successful than international terrorist plots.

---

[429] Lewis, James A. "Assessing Counterterrorism, Homeland Security, and Risk." *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 83-97. Print.
[430] Ibid.
[431] Ibid.

Policymakers, therefore, must shift focus from hardening a long list of critical assets to a more pragmatic approach that recognizes the inherent randomness of any domestic terrorist attack. For example, policymakers could reallocate federal funds to strengthen telecommunications systems that are used by every major component of the U.S. energy industry, instead of hardening individual nodes within the system. Additionally, policymakers could spend more on first-responders for vulnerable areas, as opposed to hardening bridges, buildings, and other lower-profile potential targets. Essentially, these examples demonstrate a shift away from preventing individual attack scenarios towards strengthening broader vulnerabilities (like cyber and communication network) and towards creating robust response capabilities.

Likewise, policymakers must understand that threat displacement occurs; i.e., when one target is hardened, terrorists can easily change targets. Thus, there is no automatic net gain to national security from strengthening security measures at individual nodes; this is true even for some assets designated as critical infrastructure. There may be a benefit from strengthening nodes if those nodes are of particular national significance, but for generic valuable assets, the net gain is negligible. The law of threat displacement indicates that hardening one target can make another target effectively less safe. For example, if a terrorist discovers that Seattle's Space Needle has been hardened by DHS grant funding, then that terrorist will not endanger the success of her attack by pursuing the Space Needle as her target; she will change targets. This means that increased security for one asset makes other potential targets actually less safe. To be clear, "less safe" refers to the fact that other Seattle assets, to continue the example, are now more

likely to be chosen as the target of a terrorist attack than they were before the Space Needle was hardened.

Threat displacement, however, is not an argument in favor of doing nothing. Regardless of what actions are taken to protect the Space Needle, the baseline threat is unchanged: a terrorist plans to attack Seattle. The significance of threat displacement, therefore, is not that hardening one target *increases* risk, but rather that hardening a target does not *eliminate* risk, and may not even *reduce* risk. Hardening targets merely transfers risk. Once policymakers understand threat displacement, they must then utilize a kind of security calculus to determine whether there is a net gain from displacing risk from one target to others. To return to an earlier example, policymakers may decide that the Space Needle has significant national importance (economically, politically, or in terms of morale), and that for that reason, there is value in displacing the risk of a terrorist event targeting the Space Needle to other assets in Seattle.

This first phase of the necessary mental calculus is straightforward; all that must be determined is if there is extraordinary inherent value associated with specific targets. The value of a target is determined not only by its national significance, but also based on the potential loss of life and economic impact if the target were attacked. The second phase of security calculus is more complex. Once policymakers identify a target as worth protecting, they must make an effort to quantify the value of protecting that target. How much should the United States be willing to pay to prevent the Space Needle from being attacked? This is a difficult exercise since most of the benefits derived from safeguarding specific assets are intangible. In other words, how do you quantify the value of the Statue of Liberty? The Statue of Liberty has some economic value as a tourist attraction, but the

indisputable value of that asset stems from its poignancy as a national icon, and from the adverse effect on national morale any attack on the Statue of Liberty would have. While quantifying value is difficult, it must be addressed, since there has to be a ceiling for the inherent value of national icons to guide federal spending for protective measures.

Similarly, policymakers must also distinguish two other types of targets when allocating funds for protective measures. First, there are a number of targets considered vulnerable, in that they are easy to attack, but yet are not vulnerable in that they are easy to replace if attacked.[432] There are implicit consequences for terrorist attacks, such as the shock to the national collective psyche, but beyond these unquantifiable consequences, many pieces of critical infrastructure cost more to protect than they would cost to rebuild.

The second type of targets that policymakers must differentiate are targets for which adequate protection would mean shutting down the asset entirely.[433] For example, public transportation systems are risk-laden modes of transportation since they are, by definition, easily accessible and open to the public without mechanisms to prevent access by potentially dangerous individuals. There is no way to remove the risk of terrorism for public transportation systems without fundamentally changing the purpose and nature of public transportation. Enacting the necessary security measures, such as screening all passengers before they enter the public transportation vehicle, is untenable since enacting them would require either unsustainably high federal investments, or a massive increase in the price of using public transportation. The first option is not possible given the finite nature of security funds, and the second option is not possible because it would ruin

[432] Mueller, John "Assessing Measures Designed to Protect the Homeland." *Terrorizing Ourselves: Why U.S. Counterterrorism Policy is Failing and How to Fix It*. Washington, D.C.: CATO Institute, 2010. 99-119. Print.
[433] Ibid.

public transportation whose consumer base opts to use a less convenient mode of transportation, relative to personal car ownership, because of the financial gains mass transit offers. Thus, there is no way to secure mass transit without crippling the system. This is just one example of the sort of industry policymakers must recognize as having inextricable security limitations.

In short, this thesis does not necessarily advocate less spending, so much as it advocates a more nuanced approach to spending that limits worst-case scenario thinking and focuses on realistic prevention and creating resiliency. The first consequence of this modality of thinking about security spending is to avoid addressing unrealistic threats. Atomic terrorism, if successful, would be horrific. However, the likelihood of a terrorist organization obtaining a nuclear weapon, yet alone transporting it and detonating it successfully, is severely limited. American security expenditures should reflect this limitation, not the worst-case scenario. A more nuanced approach to security spending would also attempt to incorporate the negative externalities detailed in Chapter Two. Several security sectors, such as intelligence, have significant negative externalities. These costs, such as curtailed civil liberties, are not quantifiable but that does not mean that they can be ethically discounted in security calculations.

Additionally, policymakers must understand that there is a double-cost (or a double-benefit) for many security measures. The first cost is the initial cost to the American taxpayer for whatever security programs are allocated from federal funds; and the second cost stems from the economic costs of security measures to businesses and individual consumers. More specifically, security measures increase cost to private business, thus increasing the market price for commerce for that industry. This increase is

either absorbed by the corporation as a loss, or is passed on to consumers by way of price increases. Alternatively, there may be a double-benefit from security measures. The first benefit is an increase in personal and national security from a specific anti-terrorism measure, and the second benefit is the stimulatory effect of security measures on certain segments of the economy. Whether there is a double-cost or a double-benefit, federal measures have a direct effect on private business and individual consumers that is often excluded from policymakers' decision to legislate security regulations. These costs are often discounted or underestimated because the economic effects of legislation are felt much later as an echo of regulation.

Instead of a straight cost-benefit analysis, homeland security expenditures should be subject to a systematic, dynamic scoring process that takes into account risk, cost, possible positive and negative externalities, other federal budget priorities, and the marginal gain from each security initiative. This scoring process would evaluate risk by giving each risk sector a score based on the likelihood and potential consequences of an attack. Then security efforts in each risk sector would be scored based on positive and negative externalities and on marginal program benefit (how efficiently and effectively does the program address risk?) Then federal funds would be allocated based on each programs' score. This scoring mechanism would standardize the appropriations process for homeland security to avoid wasteful spending. It is also important to appropriate homeland security funds systematically because of the lack of transparency in this sector. Taxpayers do not have access to operational information about security programs and, thus, a standard appropriations process based on rational, dispassionate methods would at least assure taxpayers that their tax dollars are being allocated reasonably.

The original purpose of this paper was to conduct a crude risk-cost-benefit analysis in an attempt to determine if the U.S. homeland security strategy was successful (defined as efficiently addressing risk). In pursuit of that objective, however, this thesis has also taken on a second, and perhaps more important purpose: to determine what information about risk, cost, and benefit is available to the average American. Risk is well documented; a large body of work defining the threat of terrorism for the United States is available from a host of sources and issue experts. Cost is piecemeal, but mostly discernable for the tenacious inquirer, assuming that she is willing to troll various Internet sources to form an amalgamation of funding data. But there is simply no way to appreciate the benefit of U.S. homeland security measures without intelligence information. Moreover, there is no way to know what else would be done with the federal funds saved if homeland security funding was reduced. There is also no non-arbitrary way to deal with certain social costs (like reduced civil liberties) from increase security, and there is also no way to know the extent of the economic effects (both positive and negative) of security efforts. Thus, the role for economic analysis in anti-terrorism appropriations is limited.

With respect to the second purpose of this thesis— discovering what information is publically available and the quality of that information— all that can be determined definitively from public information is that the U.S. homeland security strategy places intelligence as the highest priority, probably over-protects against the low-probability threat of atomic terrorism, is vulnerable to cyberterrorism and bioterrorism, and lacks transparency with respect to program-specific costs and benefits. Interestingly, the process of conducting a risk-cost-benefit analysis revealed little about the success of the

U.S. homeland security strategy, but revealed a great deal about the lack of transparency for U.S. anti-terrorism measures. There are only two ways to improve homeland security transparency: (1) make public the operational information for anti-terrorism programs so that the effectiveness of security efforts is determinable; or (2) establish a metric for scoring security programs (like the process detailed above) so that there is a metric to determine the value of each security program and of security spending generally. The former option is unrealistic because declassifying operational information could jeopardize anti-terrorism efforts and endanger national security. Thus, installing a metric to gauge the effectiveness of security spending is the necessary compromise to inform Americans about anti-terrorism efforts without compromising homeland security. Once value is determinable, taxpayers can finally make normative judgments about the success of the U.S. homeland security strategy.

Work Cited

9/11 Commission Report. The National Commission on Terrorist Attacks Upon the United States, Web. 14 Apr. 2011. <http://govinfo.library.unt.edu/911/report/index.htm>.

An Act Making Appropriations for Energy and Water Development and Related Agencies for the Fiscal Year Ending September 30, 2010, and for Other Purposes. PUBLIC LAW 111–85—OCT. 28, 2009. Web. 10 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ85/pdf/PLAW-111publ85.pdf>.

Archick, Kristin, et al. *European Approaches to Homeland Security and Counterterrorism*. Congressional Research Service, 24 July 2006. Web. 30 Mar. 2011. <http://www.hlswatch.com/sitedocs/RL33573.pdf>.

Boyd, Dallas, Lewis A. Dunn, and James Scouras. "Why Has the United States Not Been Attacked Again?" *The Washington Quarterly* (July 2009). pag. *Informaworld*. Web. 16 Apr. 2011 <http://www.informaworld.com/smpp/content~db=all~content=a912817415>.

Budget authority for DOE programs granted through a series of four continuing resolutions available online through the Library of Congress *Thomas* Website: "Status of Appropriations Legislation for Fiscal Year 2007." *Thomas*: Library of Congress.Web.10 Mar. 2011. <http://thomas.loc.gov/home/approp/app07.html>.

CHALK, PETER. *Hitting America's Soft Underbelly The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*. The Rand Corporation. 3 Mar. 2011. <http://www.rand.org/pubs/monographs/2004/RAND_MG135.pdf>.

Chalk, Peter, Hoffman, Bruce, Reville, Robert T., Kasupski, Anna-Britt. *Trends in Terrorism:Threats to the United States and the Future of the Terrorism Risk Insurance Act. RAND Corporation.* 2005. Web. 14 Apr. 2011. <http://www.rand.org/pubs/monographs/MG393.html>.

Chantrill, Christopher. "FY2010 Government Spending Details ." *U.S. Government Spending*. Web. 10 Apr. 2011. <http://www.usgovernmentspending.com/piechart_2010_US_fed>.

Chertoff, Michael. *Homeland Security: Assessing the First Five Years*. Philadelphia: University of Pennsylvania Press, 2009. Print.

"The Comprehensive National Cybersecurity Initiative." *National Security Council*, The White House.Web. 14 Mar. 2011. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

Consolidated Appropriations Act, 2008. H.R.2764 -December 26, 2007. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgibin/query/z?c110:H.R.2764.enr:

D'Agostino, Davi M. *Weapons of Mass Destruction: Actions Needed to Track Budget Execution for Counterproliferation Programs and Better Align Resources with Combating WMD Strategy*. Government Accountability Office, 28 Sept. 2010. Web. 10 Mar. 2011. <http://www.gao.gov/new.items/d10755r.pdf>.

Department of Homeland Security Appropriations Act, 2007. H.R.5441- October 4th, 2006. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.5441.enr:

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS ACT, 2010. PUBLIC LAW 111–83-OCT. 28, 2009.*Thomas*, Library of Congress. 1 Mar. 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ83/pdf/PLAW-111publ83.pdf>.

The Department of Homeland Security. *Update on Implementation of the Chemical Facility Anti-Terrorism Standards and Development of Ammonium Nitrate Regulations*. 2010 Chemical Sector Coordinating Council Security Summit. http://www.dhs.gov/xlibrary/assets/chemsec_summit_2010_cfats%20update_sue_armstrong.pdf

Drakos, Konstantinos, and Nicholas Giannakopoulos. *An econometric analysis of counterterrorism effectiveness: the impact on life and property losses*. Public Choice, Nov. 2008. Web. 15 Apr. 2011. <http://www.springerlink.com/content/n5537u4918n3274l/>.

Fainberg, Anthony. "The Terrorist Threat to Inbound U.S. Passenger Flights: Inadequate Government Response." *Homeland Security Affairs: The Journal of the Naval Postgraduate School Center for Homeland Defense and Security.* 3 Mar. 2011. <http://www.hsaj.org/?article=5.1.5>

Gulliver. "Full-Body Scanners: Which American airports have the new full-body scanners?" *The Economist*. 23 Dec. 2010.

Harmon, Christopher, Andrew Pratt, and Sebastian Gorka. *Toward a Grand Strategy Against Terrorism*. New York: McGraw-Hill, 2011. Print.

H.R.1105—Omnibus Appropriations Act, 2009. *Thomas*: Library of Congress, Web. 10 Mar. 2011. <http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.1105.enr:>.

H.R. 2611 A bill to amend the Homeland Security Act of 2002 to authorize the Securing the Cities Initiative of the Department of Homeland Security, and for other

purposes. CONGRESSIONAL BUDGET OFFICE, Dec. 2009. Web. 16 Apr. 2011. <http://www.cbo.gov/ftpdocs/108xx/doc10848/hr2611.pdf>.

H.R.2764— Consolidated Appropriations Act, 2008. *Thomas*: Library of Congress, Web.10 Mar. 2011. http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.2764.enr:

Jenkins, William O., Jr. *BIOSURVEILLANCE Preliminary Observations on Department of Homeland Security's Biosurveillance Initiatives*. *Government Accountability Office.* July 16, 2008. Web. 10 Mar. 2011. <http://www.gao.gov/new.items/d08960t.pdf>.

JINDAPON, PAAN, and WILLIAM S. NEILSON. *THE IMPACT OF SOCIETAL RISK ATTITUDES ON TERRORISM AND COUNTERTERRORISM*. Journal of Economics and Politics , Nov. 2009. Web. 15 Apr. 2011. <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0343.2009.00360.x/abstract>.

Katzman, Kenneth. *Al Qaeda in Iraq: Assessment and Outside Links* . Congressional Research Service, 15 Aug. 2008. Web. 31 Mar. 2011. <http://www.fas.org/sgp/crs/terror/RL32217.pdf>.

LaFree, Gary, Sue-Ming Yang, and Martha Crenshaw. *Trajectories of Terrorism: Attack patterns of foreign groups that have targeted the United States, 1970–2004*. Stanford University, Web. 31 Mar. 2011. <http://iis-db.stanford.edu/pubs/22662/Crenshaw_Trajectories_of_terrorism.pdf>.

Mueller, John Mueller, and Mark G. Stewart. "Hardly Existential: Thinking Rationally About Terrorism." *Foreign Affairs* (Apr. 2010). Web. 14 Apr. 2011.<http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential?page=show>.

Nacos, Brigitte L. *Terrorism and Counterterrorism: Understanding Threats and Responses in the Post 9/11 World*. 3rd ed. New York, NY: Penguin Academics, 2009. Print.

National Counterterrorism Center 2008 Report on Terrorism. Web. 5 Apr. 2011. <http://www.fas.org/irp/threat/nctc2008.pdf>.

National Emergency Communications Plan. The Department of Homeland Security. Web. 14 Mar 2011. <http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf>.

The National Nuclear Security Administration. The U.S. Department of Energy, Mar. 2011. Web. 10 Mar. 2011. <http://nnsa.energy.gov/>.

North American Electric Reliability Corporation. Web. 13 Mar. 2011. <http://www.nerc.com/index.php>.

Office of Management and Budget. *Budget of the United States Government, Fiscal Year 2012*. The White House, President Barack Obama. Web. 14 Apr. 2011. <http://www.whitehouse.gov/omb/budget/Overview/>.

"Office of the Coordinator for Counterterrorism." *The U.S. Department of State*. Web. 31 Mar. 2011. <http://www.state.gov/s/ct/index.htm>.

Omnibus Appropriations Act, 2009. H.R.1105- September 30, 2009. *Thomas*, Library of Congress. 1 Mar. 2011. http://thomas.loc.gov/cgibin/query/C?c111:./temp/~c111mTqKDx

Preble, Christopher. "Toward a Responsible Defense Budget." *CATO Institute*. 30 June 2010. Web. 16 Apr. 2011. <http://www.cato.org/pub_display.php?pub_id=11946>.

Priest, Dana, and William Arkin. "Top Secret America ." *The Washington Post* 19 July 2010. *The Washington Post* . Web. 16 Apr. 2011. <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>.

ROGGIO, BILL. "Senior al Qaeda in Iraq leader killed in Miqdadiyah." *The Long War Journal*. 16 Jan. 2008. Web. 31 Mar. 2011.<http://www.longwarjournal.org/archives/2008/01/senior_al_qaeda_in_i_1.php>.

Sandler, Todd. "Terrorism and Policy: Introduction." *Journal of Conflict Resolution* (Dec. 2009). pag. *SAGE*. Web. 15 Apr. 2011. <http://jcr.sagepub.com/>.

Stewart, M.G., and J. Mueller. *Assessing the Costs and Benefits of United States Homeland Security Spending*. CENTRE FOR INFRASTRUCTURE PERFORMANCE AND RELIABILITY. Web. 16 Apr. 2011. <http://polisci.osu.edu/faculty/jmueller/stewarr1.pdf>.

Stewart, Mark G. "Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure." *The International Journal of Critical Infrastructure Protection* (2009). pag. *Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia*. Web. 15 Apr. 2011. <http://STEWJCIP.PDF>.

Terrorism and Homeland Security: Thinking Strategically About Policy. Ed. Paul Viotti, Michael Opheim, and Nicholas Bowen. Boca Raton, FL: CRC Press, Taylor and Francis Group, 2008. Print.

Transportation Security Administration. Department of Homeland Security. Web. 12 Mar. 2011. <http://www.tsa.gov/index.shtm>.

United States Department of Energy, and United States Department of Homeland Security. *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010*.Web.13 Mar. 2011.
< http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_2010.pdf>

The U.S. Department of Homeland Security. *The National Response Framework.* Jan. 2008. Web. 5 Mar. 2011. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

The U.S. Nuclear Regulatory Commission. *Performance and Accountability Report — NRC Summary of Performance And Financial Information Fiscal Year 2010.* Web. 10 Mar. 2011.
<http://www.nrc.gov/readingrm/doccollections/nuregs/staff/sr1542/v16/s1/sr1542v16s1.pdf>.

United States Secret Service. *United States Secret Service Strategic Plan (FY2008- FY2013).* U.S. Department of Homeland Security. Web. 6 Mar. 2011.
<http://www.secretservice.gov/FY09_SecretService_Annual%20Report-Web.pdf>.

United States Senate. Senate Homeland Security and Governmental Affairs Committee. *Nine Years after 9/11: Confronting the Terrorist Threat to the Homeland.* Michael Leiter, Director of the National Counterterrorism Center. September 22, 2010. Text From: *Senate Committee on Homeland Security and Governmental Affairs hearing database.* Accessed: February 20, 2011.

Zycher, Benjamin. *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*. RAND Corporation , 2003. Web. 15 Apr. 2011.
<http://www.rand.org/pubs/monograph_reports/MR1693.html>.